MASTER'S THESIS

Beschermen tegen bedreigingen van binnenuit

Het voorkomen en mitigeren van insider threats met behulp van Identity & Acces Management

Janga, E.C. (Ezzard)

Award date:
2019

Beschermen tegen bedreigingen van binnenuit

Het voorkomen en mitigeren van insider threats met behulp van Identity & Access Management.

Defending against the threat from within

Preventing and mitigating insider threats by using Identity & Access Management.

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeertraject Business Process Management and IT
Student:	Ezzard Janga
Identiteitsnummer:	
Datum:	10 augustus 2019
Afstudeerbegeleider:	prof. dr. Lex Bijlsma
Meelezer:	dr. Lloyd Rutledge
Examinator:	dr. Lloyd Rutledge
Versienummer:	1.0
Status:	Definitief

Abstract
Organisaties werken continu aan adequate en robuuste informatiebeveiliging. Tegelijkertijd worden de aanvallen door kwaadwillende partijen en individuen ook steeds geavanceerder. Ook nu ontstaat weer een nieuwe trend waarbij aanvallen steeds vaker van binnenuit worden geïnitieerd. Dit soort bedreigingen worden ook wel insider threats genoemd. Een voorbeeld van een insider threat is een interne medewerker met bewuste kwaadaardige bedoelingen. Echter, insider threats zijn lang niet altijd alleen medewerkers met kwaadaardige bedoelingen. Voorbeelden van gedrag dat onbewust of onbedoeld tot een bedreiging kan leiden zijn onder andere het werken vanaf een externe locatie via een onbeveiligde internetverbinding of het slachtoffer worden van diefstal van bedrijfsapparatuur, zoals een laptop of mobiele telefoon. Uit een recent onderzoek blijkt het dat organisaties insider threats steeds serieuzer nemen, maar het ook lastig vinden om te managen. Oplossingen worden met name gezocht in Data Loss Prevention, data encryptie en Identity & Access Management.

Dit onderzoek is gericht op het onderzoeken van het effect van Identity & Access Management op insider threats en is bedoeld om antwoord te geven op de vraag: welke beveiligingsmaatregelen uit het aandachtsgebied Identity & Access Management verlagen daadwerkelijk de kans op en impact van beveiligingsincidenten veroorzaakt door insider threats?

Sleutelbegrippen
Identity & Access Management, informatiebeveiliging, logische toegangsbeveiliging, insider threats

Samenvatting

Informatiebeveiliging is het geheel aan activiteiten, processen en maatregelen die samen bijdragen aan het detecteren, voorkomen en mitigeren van aanvallen op computersystemen, netwerken en informatie. Hoewel organisaties steeds beter worden in het zorgen voor adequate en robuuste informatiebeveiliging, worden de aanvallen door kwaadwillende partijen en individuen ook steeds geavanceerder. Nu ontstaat een nieuwe trend waarbij aanvallen steeds vaker van binnenuit worden geïnitieerd. Dit soort bedreigingen worden ook wel *insider threats* genoemd.

Het begrip *insider threat* is de Engelse benaming voor een bedreiging van binnenuit. Een voorbeeld hiervan is een interne medewerker met bewuste kwaadaardige bedoelingen. Echter, insider threats zijn lang niet altijd alleen medewerkers met kwaadaardige bedoelingen. Voorbeelden van het gedrag dat onbewust of onbedoeld tot een bedreiging kan leiden zijn onder andere het werken vanaf een externe locatie via een onbeveiligde internetverbinding of het slachtoffer worden van diefstal of het verlies van bedrijfsapparatuur, zoals een laptop of mobiele telefoon. Uit een recent onderzoek blijkt het dat organisaties insider threats steeds serieuzer nemen, maar het tegelijkertijd ook lastig vinden om te managen. Oplossingen worden met name gezocht in Data Loss Prevention, data encryptie en Identity & Access Management.

Dit onderzoek is gericht op het onderzoeken van het effect van Identity & Access Management op insider threats en is bedoeld om een antwoord te geven op de volgende centrale hoofdvraag:
"Welke beveiligingsmaatregelen uit het aandachtsgebied Identity & Access Management verlagen daadwerkelijk de kans op en impact van beveiligingsincidenten veroorzaakt door insider threats?"

Het onderzoek is opgesplitst in twee onderdelen, namelijk een literatuuronderzoek en een empirisch onderzoek. In het een literatuuronderzoek wordt op basis van zes deelvragen antwoord gegeven op de soorten insider threats die zich voor kunnen doen, wat de kenmerkende onderdelen zijn van het aandachtsgebied Identity & Access Management, wat de veelvoorkomende beveiligingsincidenten zijn die door insider threats worden veroorzaakt, wat voor impact ze kunnen hebben op de getroffen organisatie en welke maatregelen van Identity & Access Management een positief effect hebben op het verlagen van de kans op en impact van beveiligingsincidenten veroorzaakt door insider threats. De resultaten van het literatuuronderzoek zijn vervolgens gebruikt als het theoretisch kader voor het tweede deel van het onderzoek, namelijk het empirisch onderzoek.

Voor het empirische deel van het onderzoek is gekozen voor een meervoudige case study. Hierbij zijn drie cases onderzocht waarbij sprake was van een **bewuste** insider threat. Binnen de kaders van dit onderzoek is ervoor gekozen om alle cases te beperken tot gebeurtenissen in de financiële sector. De incidenten moesten daarnaast in de laatste 5 jaar zijn voorgekomen en de dreiging moest altijd precies één medewerker betreffen. Kortom, incidenten waarbij twee of meer personen samen hebben gehandeld waren uitgesloten. Van elke case is vastgesteld (1) wat was de aard van het incident, (2) op welke wijze is misbruik gemaakt van (vertrouwelijk) bedrijfsinformatie, (3) met welk doel handelde de medewerker, (4) wat voor risico's heeft de dader moeten nemen, (5) hoe en wanneer is het incident gedetecteerd, (6) wat voor IAM-maatregelen waren destijds ingericht, (7) wat voor maatregelen zijn na de evaluatie van het incident genomen en (8) wat voor IAM-maatregelen hadden dit incident kunnen voorkomen?

Uit de resultaten vanuit het literatuuronderzoek blijkt dat de meest voorkomende incidenten die door insider threats veroorzaakt worden met name gericht zijn op het oneigenlijk gebruikmaken of het uitlekken van (vertrouwelijke) bedrijfsinformatie. Hierbij zijn insider threats onder te verdelen in twee categorieën, namelijk de bewuste gevallen en de onbewuste gevallen. Volgens de theorie ontstaan de bewuste gevallen zich bij de juiste combinatie van motivatie en kansen die samen tot een actie leiden. Binnen de financiële sector is het de kans op financieel gewin dat tot actie leidt. Bij andere sectoren is het motief niet altijd financieel van aard, maar wel bedoeld om een persoonlijk voordeel te behalen. Pas daarna volgen andere motieven zoals wraak, stress en bewuste sabotage.

Uit de conclusie blijkt dat de beveiligingsmaatregelen uit het aandachtsgebied van Identity & Access Management een wisselend effect hebben op het daadwerkelijk verlagen van de kans op en impact van beveiligingsincidenten die veroorzaakt worden door insider threats. De theorie en de praktijk wijzen beiden uit dat bepaalde IAM-maatregelen, zoals de periodieke herbeoordeling van uitgegeven autorisaties en het herzien van autorisaties bij interne verplaatsingen, een positief effect hebben op het voorkomen dat medewerkers toegang krijgen tot vertrouwelijke bedrijfsinformatie dat niet relevant is voor het uitvoeren van hun dagelijkse werkzaamheden. Ook het onbedoeld en ongewenst stapelen van conflicterende autorisaties, zodat medewerkers bijvoorbeeld in staat zijn om zelfstandig facturen in te voeren en goed te keuren, kan hiermee worden voorkomen. Maatregelen zoals het vierogenprincipe en het scheiden van taken en bevoegdheden bij kritische en/of fraudegevoelige handelingen hebben ook een positief effect op het voorkomen dat een medewerker die alleen handelt in staat is om misbruik te maken van bedrijfsinformatie.

Echter, wanneer een medewerker met legitieme redenen toegang heeft tot (vertrouwelijke) bedrijfsinformatie, is de effectiviteit van IAM-maatregelen vrij beperkt. In dit soort gevallen is het noodzakelijk om IAM te combineren met andere soorten maatregelen en technieken om de kans op een incident door een insider threat te kunnen verlagen. Zoals het toepassen van data-abstractie of het continu monitoren op afwijkingen in de bedrijfsvoering met slimme oplossingen zoals Data Loss Prevention en Security Information & Event Management (SIEM).

Het verlagen van de kans op een bewuste insider threat kan ook met niet-technische oplossingen. Uit het literatuuronderzoek en de case study is gebleken dat het motief in de financiële sector vaak het persoonlijke financiële gewin is. De overweging of verleiding om tot actie over te gaan hangt nauw samen met drie factoren, namelijk de vereiste inspanning, de eventuele risico's (zoals de pakkans) en de verwachte opbrengsten. Door deze factoren te beïnvloeden, bijvoorbeeld door als organisatie de risico's en consequenties veel prominenter te benadrukken, kan dit potentieel een afschrikkend effect hebben op de overweging van een insider threat om daadwerkelijk tot actie over te gaan.

Summary

Information security is the whole of all activities, processes and measures that together contribute to the detection, prevention and mitigation of attacks on computer systems, networks and information. While organizations are increasingly becoming better at making sure their information security is adequate and robust, the attacks initiated by malicious groups and individuals are also increasingly becoming more sophisticated. Now a new trend is emerging in which attacks are now more often than before being initiated from within. These types of threats are also known as *insider threats*.

The term insider threat is used for a threat which comes from within. An example of such a threat is an internal employee with deliberate malicious intent. However, an insider threat is not always an employee with malicious intent. The kind of behavior that can unknowingly or unintentionally lead to a threat are for example, working from a remote location via an unsecured internet connection or being the victim of theft or loss of company equipment such as a laptop or mobile phone. A recent study shows that organizations are taking insider threats more seriously, but also find it to be quite difficult to manage. Solutions are mainly being sought in Data Loss Prevention, data encryption and Identity & Access Management.

This research is aimed at investigating the effects of Identity & Access Management security measures on insider threats and is meant to provide an answer to the following main question: ***"Which security measures in the Identity & Access Management focus area actually reduce the chance and impact of security incidents caused by insider threats?"***

The research is divided into two parts, a literature study and an empirical study. In the literature study, sub-questions were defined that together give insight in the types of insider threats that could occur, what the key components of Identity & Access Management are, what the common security incidents are that are caused by insider threats, what the impact of such security incidents could have on an organization and which Identity & Access Management security measures have a positive effect on reducing the chance and impact of security incidents caused by insider threats. The result of the literature study is then used as the theoretical framework for the second part of the research, which is the empirical research.

The empirical research was done by performing a multiple case study. Three cases were investigated in which there was an insider threat with **deliberate** malicious intent. For this research, the decision was made to limit the cases to only events that occurred in the financial sector. In addition to that, the incidents must have happened in the last 5 years and the incident must have been initiated by a single employee. In other words, incidents where multiple persons worked together were excluded. For each case it was determined (1) what was the nature of the incident, (2) how was (confidential) company information misused, (3) what was the culprit's purpose, (4) which risks did the culprit take, (5) how and when was the incident detected, (6) what type of IAM security measures could have prevented the incident?

The results of the literature study show that the most common incidents caused by insider threats are mainly related to the misuse or leaking of (confidential) company information. Insider threats can be divided into two categories: the intentional threats and the unintentional threats. According to the theory, intentional threats form when the right combination of motivation and opportunities come together, which then might lead to an action. Within the financial sector, the opportunity for personal financial gain is often the motivation that leads to an action. Within other sectors, the motive is not always financial in nature, but is still meant to somehow achieve some kind of personal benefit. Only then do other motives follow such as revenge, stress or sabotage.

The conclusions show that the security measures from the Identity & Access Management focus area have a varying effect on reducing the chance and impact of security incidents caused by insider threats. The theory and the reality both show that certain IAM measures, such as periodic review of all authorizations and access reviews during internal job changes have a positive effect on preventing employees from unintentionally having access to (confidential) company information that is not relevant to their work. This can also prevent employees from potentially stacking and having conflicting authorizations, so that, for example, an employee would be able to independently submit and approve the payment of an invoice. Taking measures such as the four-eyes principle and separation of duties for critical activities or tasks that are susceptible to fraud also have a positive effect on preventing an employee from being able to act alone or misuse company information.

However, the moment that an employee has legitimate reasons to access (confidential) company information, the effectiveness of IAM measures is reduced significantly. In such cases it is necessary to combine IAM with other kinds of measures and techniques that reduce the chance of a security incident by an insider threat. This would be, for example, applying data abstraction or continuous monitoring for deviations in business operations with smart solutions such as Data Loss Prevention and Security Information & Event Management (SIEM).

Non-technical solutions can also help reduce the chance of an incident caused by an insider threat with malicious intent. The literate study and the empirical study have both shown that the motive in the financial sector is often linked to personal financial gain. The consideration or temptation for acting are closely linked to three factors, namely the required effect, the potential risk (such as the chance of being caught) and the expected returns. By influencing these factors, for example, by emphasizing the risks and consequences more prominently, this could potentially have a deterrent effect on an insider threat that's considering to act.

Inhoudsopgave

1. Introductie

1.1 Achtergrond

Informatiebeveiliging is het geheel aan activiteiten, processen en maatregelen die samen bijdragen aan het detecteren, voorkomen en mitigeren van aanvallen op computersystemen, netwerken en informatie. Het vakgebied van informatiebeveiliging is dan ook complex, dynamisch en steeds in ontwikkeling. Hoewel organisaties steeds beter worden in het zorgen voor adequate en robuuste informatiebeveiliging, worden de aanvallen door kwaadwillende partijen en individuen ook steeds geavanceerder. In de afgelopen jaren is met name het belang en niveau van informatiebeveiliging binnen organisaties steeds beter geworden. Dit komt vooral door het implementeren van nieuwe (technische) oplossingen en organisatorische maatregelen waarmee men proactief bedreigingen weet te detecteren, voorkomen en mitigeren. Tegelijkertijd ontstaat juist nu een nieuwe trend waarbij aanvallen steeds vaker van binnenuit worden geïnitieerd. Dit soort bedreigingen worden ook wel *insider threats* genoemd. Binnen het vakgebied van informatiebeveiliging is op wetenschappelijk niveau nog beperkt onderzoek gedaan naar het voordoen en voorkomen van aanvallen veroorzaakt door deze bedreigingen van binnenuit.

1.2 Gebiedsverkenning

Het vakgebied van informatiebeveiliging is breed en divers. Hierdoor zijn ook de meningen verdeeld over wat informatiebeveiliging is en wat het anders maakt dan *cybersecurity* of *securitymanagement*. In dit onderzoek kunnen deze termen door elkaar heen worden gebruikt, echter wel ten alle tijden met dezelfde betekenis en definitie, namelijk:

> *Informatiebeveiliging gaat over de maatregelen en procedures om beschikbaarheid, exclusiviteit en integriteit van informatievoorziening te garanderen en in het bijzonder om de continuïteit van de informatie en informatievoorziening te waarborgen en de gevolgen van incidenten tot een acceptabel niveau te beperken.* (van den Berg, 2015)

Informatiebeveiliging kan worden onderverdeeld in verschillende aandachtsgebieden. Eén van deze aandachtsgebieden is Identity & Access Management (IAM). Identity & Access Management is het geheel aan beleid, procedures en processen omtrent het authentiseren en autoriseren van personen binnen de IT-omgeving van een organisatie (Gunter, Liebovitz, & Malin, 2011). Binnen IAM zelf is het ook nog mogelijk om onderscheid te maken tussen Enterprise IAM en Customer IAM. Enterprise IAM is vooral gericht op het beheren en verstrekken van autorisaties van interne medewerkers. Customer IAM gaat dan juist weer over het beheren en verstrekken van autorisaties voor externe partijen die toegang hebben of willen tot de interne informatiesystemen van een organisatie.

Het begrip *insider threat* is de Engelse benaming voor een bedreiging van binnenuit. Een voorbeeld hiervan is een interne medewerker met bewuste kwaadaardige bedoelingen. Echter, insider threats zijn lang niet altijd alleen medewerkers met kwaadaardige bedoelingen. Enkele voorbeelden van het gedrag dat onbewust of onbedoeld tot een bedreiging kan leiden zijn onder andere het per ongeluk versturen van vertrouwelijke informatie naar een verkeerde geadresseerde, het werken vanaf een externe locatie via een onbeveiligde internetverbinding of het slachtoffer worden van diefstal of het verlies van bedrijfsapparatuur, zoals een laptop of mobiele telefoon ("The Insider Threat," 2017).

1.3 Probleemstelling

In 2017 heeft het SANS Institute (Cole, 2017) een onderzoek gedaan naar in hoeverre organisaties voorbereid zijn op een aanval geïnitieerd of ondersteund door het eigen personeel (insiders). Uit dit onderzoek is gebleken dat maar liefst 45% van de onderzochte organisaties niet bewust is van de consequenties die kunnen volgen door beveiligingsincidenten waarbij een insider betrokken is. In 33% van de gevallen konden ze zelfs niet eens inschatten wat de verwachte impact zou zijn als de organisatie het slachtoffer zou zijn van een dergelijk incident. Uiteindelijk bleek ook dat slechts 18% van de respondenten een plan van aanpak had om met de dreiging van insider threats om te gaan.

In een ander rapport over een onderzoek onder 472 cybersecurity professionals (Schulze, 2018) gaf 90% van de respondenten aan dat ze het gevoel hadden dat hun organisatie zeer kwetsbaar is voor insider threats. Hoofdzakelijk verwijten ze dit aan te veel gebruikers met overtollige bevoegdheden, het groeiende aantal (mobiele) apparaten die toegang hebben tot vertrouwelijke informatie en de groeiende complexiteit van IT in het algemeen.

1.4 Opdrachtformulering

Uit een recent onderzoek blijkt het dat organisaties insider threats steeds serieuzer nemen, maar het tegelijkertijd ook lastig vinden om te managen (Schulze, 2018). Deze waarneming is niet beperkt tot een specifieke branche en/of organisatiegrootte. De meeste organisaties geven wel aan al bezig te zijn met het opstellen van plannen om met insider threats om te gaan. Oplossingen hiervoor worden met name gezocht in Data Loss Prevention, data encryptie en Identity & Access Management.

Dit onderzoek is beperkt tot het onderzoeken van het effect van Identity & Access Management op insider threats en is bedoeld om een antwoord te geven op de volgende centrale hoofdvraag:
"Welke beveiligingsmaatregelen uit het aandachtsgebied Identity & Access Management verlagen daadwerkelijk de kans op en impact van beveiligingsincidenten veroorzaakt door insider threats?"

Het eerste deel van het onderzoek bestaat uit een literatuuronderzoek waarin antwoord wordt gegeven op volgende deelvragen:

1. Wat zijn de verschillende soorten insider threats binnen de informatiebeveiliging?
2. Wat zijn de kenmerkende onderdelen van Identity & Access Management?
3. Wat zijn de veelvoorkomende beveiligingsincidenten veroorzaakt door insider threats?
4. Wat voor impact hebben de beveiligingsincidenten veroorzaakt door insider threats?
5. Welke maatregelen uit het aandachtsgebied Identity & Access Management verlagen de kans op het voorkomen van beveiligingsincidenten veroorzaakt door insider threats?
6. Welke maatregelen uit het aandachtsgebied Identity & Access Management verlagen de impact van beveiligingsincidenten veroorzaakt door insider threats?

Het is essentieel om eerst inzicht te krijgen in de soorten insider threats die zich voor kunnen doen. Dit wordt opgevolgd door het aandachtsgebied Identity & Access Management te onderzoeken om de kenmerkende onderdelen hiervan in kaart te brengen. Op basis hiervan wordt onderzocht wat de veelvoorkomende beveiligingsincidenten zijn die door insider threats worden veroorzaakt en wat voor impact ze op de getroffen organisatie kunnen hebben. Uiteindelijk worden de maatregelen van Identity & Access Management onderzocht om te bepalen of ze een positief effect hebben op het verlagen van de kans en/of impact van beveiligingsincidenten veroorzaakt door insider threats.

De resultaten uit het literatuuronderzoek worden vervolgens als het theoretisch kader gebruikt voor het tweede deel van het onderzoek, het empirisch onderzoek. Het doel van het empirisch onderzoek is om door middel van een case study te toetsen of de maatregelen uit het literatuuronderzoek ook in de praktijk daadwerkelijk een positief effect hebben op het verlagen van de kans en/of impact van de insider threats die ze volgens de theorie zouden moeten hebben.

1.5 Motivatie/relevantie

In het meest recente Insider Threat Report (Schulze, 2018) is een onderzoek gedaan naar de huidige stand van zaken betreffende insider threats in 2018. Eén van de bevindingen uit dit onderzoek is dat organisaties de kans op een aanval waarbij sprake is van een insider threat hoger inschatten (36%) dan de kans op een aanval van buitenaf (34%). De kans op beveiligingsincidenten waarbij helemaal geen sprake is van opzet staat met 30% op de derde plaats. Echter, dit soort incidenten worden over het algemeen vaak alsnog door het eigen personeel veroorzaakt of mogelijk gemaakt.

Verwacht wordt dat het aantal incidenten veroorzaakt door insider threats alleen maar verder zal gaan toenemen. Daardoor wordt het kunnen omgaan met dit soort bedreigingen steeds meer van belang. Dit onderzoek is opgezet om vast te stellen of de maatregelen uit het aandachtsgebied van Identity & Access Management als een oplossing kunnen worden gezien voor het verlagen van de kans en impact op beveiligingsincidenten veroorzaakt door insider threats.

1.6 Aanpak in hoofdlijnen

Naar aanleiding van de probleemstelling is een hoofdvraag met bijbehorende deelvragen opgesteld. In de volgende hoofdstukken wordt in eerste instantie het theoretisch kader vastgesteld waarbinnen dit onderzoek plaatsvindt. Hierin wordt tegelijkertijd ook antwoord gegeven op de deelvragen in de vorm van een literatuuronderzoek. Dit wordt opgevolgd door het hoofdstuk over de methodologie, waarbij de onderzoeksmethode van het empirisch onderzoek wordt vastgesteld ten behoeve van de validiteit en betrouwbaarheid. In het hoofdstuk dat daarop volgt zijn de resultaten van het empirisch onderzoek uitgeschreven. Uiteindelijk wordt het onderzoek afgerond met een conclusie op basis van de belangrijkste resultaten en worden aanbevelingen gedaan voor de praktijk en verdere onderzoek.

Ondanks dat het aandachtsgebied van Identity & Access Management voor een groot gedeelte uit technische oplossingen bestaat, is dit onderzoek niet gericht op het onderzoeken van de verschillen tussen de diverse soorten technische oplossingen en applicaties. De maatregelen in dit onderzoek zijn beperkt tot beleidsmatige en procesmatige maatregelen. In het geval dat alsnog een technische oplossing wordt benoemd of aangeraden, dan is dit met name bedoeld om het beleid of proces te ondersteunen.

2. Theoretisch kader

2.1 Onderzoeksaanpak

Het doel van het theoretisch kader is om als wetenschappelijk basis te dienen voor het tweede deel van het onderzoek, namelijk het empirisch onderzoek. Het theoretisch kader is opgezet door middel van een literatuuronderzoek. Per onderzoeksvraag is eerst gezocht naar relevante wetenschappelijke literatuur. Om de betrouwbaarheid en validiteit van het onderzoek te waarborgen wordt van elke zoekactie naar relevante literatuur bijgehouden hoeveel treffers zijn gevonden evenals het aantal relevante en gebruikte bronnen.

Alle zoekacties naar relevante wetenschappelijke literatuur zijn uitgevoerd in de digitale bibliotheek van de Open Universiteit of in Google Scholar. Echter, om beter inzicht te krijgen in de meest actuele trends en ontwikkelingen op het gebied van IT en informatiebeveiliging, is in sommige gevallen ook de reguliere zoekmachine van Google geraadpleegd. Bij dit soort zoekacties is uitsluitend gezocht naar literatuur gepubliceerd door gerenommeerde instellingen en instituten om zoveel mogelijk te voorkomen dat onbewezen en/of ongegronde bronnen als de waarheid worden opgevat.

Op basis van de literatuur wordt op iedere onderzoeksvraag een antwoord gegeven. Uiteindelijk wordt op basis van alle resultaten een conclusie getrokken die als het theoretisch kader dient voor het empirisch onderzoek.

2.2 Uitvoering

Hieronder volgen de tabellen met per deelvraag een overzicht van de uitgevoerde zoekacties en de daarbij gebruikte zoektermen. De kolom *resultaten* geeft het totale aantal gevonden resultaten aan. De kolom *bekeken* geeft aan van hoeveel resultaten de titel en het abstract zijn doorgenomen om te bepalen of het resultaat relevant was aan de zoekterm. Alle gevonden resultaten zijn bekeken tot op het moment dat de resultaten gevoelsmatig niet langer relevant waren aan de gebruikte zoekterm. De kolom *geanalyseerd* geeft aan van hoeveel artikelen de hoofdtekst is doorgenomen nadat ze, na het lezen van het abstract, als potentieel relevant zijn beoordeeld. Artikelen die als relevant aan het onderwerp zijn beoordeeld, zijn vrijwel direct in de bibliografie opgenomen voor eventueel gebruik later in het onderzoek. De kolom *gebruikt* geeft het aantal artikelen aan die uit de zoekactie komen en uiteindelijk ook daadwerkelijk in het onderzoek zijn gebruikt. Aanvullend hierop kan het zijn dat de verwijzingen naar andere literatuur uit de eerder geanalyseerde resultaten hebben geleid tot het ontdekken van nieuwe en additionele relevante literatuur. Dit is het ‘sneeuwbaleffect’ en betekent dat sommige van de gebruikte artikelen niet direct uit de zoekresultaten zijn voortgekomen.

Uiteindelijk zijn sommige artikelen ook bij meerdere onderzoeksvragen gebruikt of zelfs al gevonden tijdens een eerdere zoekactie. Hierdoor zijn bij de latere onderzoeksvragen soms minder zoekacties uitgevoerd dan bij de eerdere onderzoeksvragen.

Tabel 1: Zoekacties in de digitale bibliotheek van de Open Universiteit

Deelvraag	*Zoektermen*	*Resultaten*	*Bekeken*	*Geanalyseerd*	*Relevant*	*Gebruikt*
1	insider threats	56.897	70	4	3	1
	Insider threats security	33.427	60	5	2	0
	what are insider threats	56.784	30	7	5	2
2	identity and access management	411.065	30	3	1	1
	identity and access management definition	133.203	30	2	1	1
	privileged account management	69.179	30	1	1	1
	customer identity and access management	85.514	30	3	2	2
	access controls	3.504.377	50	3	2	0

Tabel 1: Zoekacties in de digitale bibliotheek van de Open Universiteit (vervolg)

Deelvraag	*Zoektermen*	*Resultaten*	*Bekeken*	*Geanalyseerd*	*Relevant*	*Gebruikt*
3	insider threat incidents	11.373	70	4	3	1
4	information classification	2.606.025	30	3	0	0
	information classification + security	228.643	30	3	2	0
	data classification + security	208.142	30	4	2	1
	impact data loss	2.461.262	20	0	0	0
	impact data loss + security	534.656	20	2	0	0
	impact data breach + security	54.320	80	7	6	2
	impact data breach + trade secrets	5.316	40	3	1	0
5	iam insider threats	255	30	9	1	1
	access management + insider threat	18.726	30	1	1	0
	identity and access management + insider threat	8.684	40	5	2	1
6	dikw data information	256	30	3	3	1

Tabel 2: Zoekacties in Google Scholar

Deelvraag	*Zoektermen*	*Resultaten*	*Bekeken*	*Geanalyseerd*	*Relevant*	*Gebruikt*
1	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
2	Identity and access management	3.840.000	40	3	1	1
	identity and access management + privileged access management	456.000	30	4	2	1
3	insider threat incidents	64.000	60	4	1	0
4	verordening 2016/679	90	20	3	2	1
5	iso27001	3.970	20	3	3	1
6	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.

2.3 Resultaten en conclusies

Hieronder volgen de resultaten van elke onderzoeksvraag inclusief de argumenten die, op basis van de gevonden literatuur, tot deze antwoorden hebben geleid. Dit wordt afgerond met een conclusie van het theoretisch kader en de gevolgen voor de rest van het onderzoek.

2.3.1 De verschillende soorten insider threats

In het Nederlands betekent het begrip *insider threat* een bedreiging van binnenuit. De definitie van een 'insider' binnen de kaders van dit onderzoek is een individu waarmee de organisatie een formele arbeidsovereenkomst is aangegaan (Wall, 2013). Vanzelfsprekend betreft dit alle medewerkers die in vaste dienst bij de organisatie zijn, maar ook andere soorten medewerkers vallen hieronder. Zo ook ingehuurd personeel, consultants en medewerkers van dienstverlenende partijen. In alle gevallen gaat het om medewerkers die vanwege hun rol of functie met legitieme redenen toegang hebben tot de interne IT-omgeving van de organisatie.

Een insider threat ontstaat nooit zomaar, vaak zijn het de omstandigheden die ertoe leiden dat een medewerker zich tot een bedreiging ontwikkeld. Belangrijk hierbij is het onderscheid tussen de bewuste dreiging en de onbewuste dreiging. In 2016 is een model ontwikkeld (Sokolowski, Banks, Dover, & Theory, 2016) waarmee voorspeld kan worden wat de kans is dat een medewerker zich zal ontwikkelen tot een bewuste bedreiging voor de informatiebeveiliging. In vrijwel alle gevallen dat dit gebeurt, blijkt een constante factor het feit te zijn dat de medewerker ontevreden is ten opzichte van de organisatie. Binnen de financiële sector is het met name de kans op financieel gewin dat tot een actie leidt. Binnen andere sectoren is het motief niet altijd financieel van aard, maar wel bedoeld om op een of andere manier een persoonlijk voordeel te behalen. Pas daarna volgen andere motieven zoals wraak, stress of bewuste sabotage.

Aan de andere kant van het spectrum staan de medewerkers die onbedoeld of zonder zich hiervan bewust te zijn een bedreiging vormen voor de informatiebeveiliging. Volgens een categorisering van de soorten bedreigingen binnen de informatiebeveiliging (Willison & Warkentin, 2013) valt hiervoor een onderscheid te maken tussen (passieve) lage risico gevallen en hoge risico gevallen. De passieve gevallen leiden vaak tot incidentele beveiligingsincidenten. Zoals het per ongeluk ingaan op phishing e-mails of het verliezen van bedrijfsapparatuur met interne informatie. De hoge risico gevallen zijn medewerkers die geen kwaadaardige bedoelingen hebben, maar wel opzettelijk het beleid omzeilen voor persoonlijke doeleinden. Een voorbeeld van dit soort nalatigheid is het extern delen van interne informatie via ongeoorloofde cloud applicaties of het versturen van bedrijfsinformatie naar een persoonlijk emailadres om vervolgens thuis verder te kunnen werken.

Zowel de lage risico gevallen als de hoge risico gevallen bestaan uit medewerkers die onbedoeld een bedreiging vormen voor de informatiebeveiliging. Onwetendheid is vaak een oorzaak, men is meestal niet bewust van het onveilige gedrag. Met name medewerkers die veel bevoegdheden hebben of met veel vertrouwelijke informatie werken vormen een hoog risicogeval (Liu & Murphy, 2015). Toch zijn deze medewerkers lang niet altijd getraind over de mogelijke risico's en bedreigingen die ze voor de organisatie kunnen zijn. In het geval dat een beveiligingsincident zich toch voordoet, dan zouden ze met adequate training ook bewust kunnen zijn van hoe te handelen om het incident te melden en de eventuele gevolgschade hiervan zo spoedig en veel mogelijk te beperken.

2.3.2 De kenmerkende onderdelen van Identity & Access Management

In de afgelopen decennia is Identity & Access Management (IAM) steeds relevanter en belangrijker geworden binnen de informatiebeveiliging (Manders-Huits, 2010). Ondanks de complexe benaming gaat IAM over het verstrekken en beheren van toegangscontrole (access control) tussen personen en de informatie, diensten of faciliteiten die ze gebruiken.

IAM wordt vaak gezien als een technologie of platform, terwijl het eigenlijk een bedrijfsproces is waarin technologie slechts een ondersteunde rol in kan vervullen. Drie centrale processen vormen de basis van IAM, namelijk identificatie/registratie, authenticatie en autorisatie (Perkins & Allan, 2005). Identificatie heeft betrekking op het initieel registreren van een individu binnen het bedrijfsdomein. Eenmaal geregistreerd kan een individu zich vervolgens authentiseren door aan te tonen dat hij is wie hij zegt te zijn. In de IT kan dit bijvoorbeeld door het invoeren van een gebruikersnaam en wachtwoordcombinatie die alleen de geauthentiseerde persoon hoort te weten. In het geval dat de authenticatie succesvol verloopt, dan zal door middel van autorisatie de individu toegang krijgen tot de daartoe geautoriseerde informatie, diensten of faciliteiten. Aanvullend hierop zijn controlerende processen vereist die gericht zijn op het borgen van de correctheid van de autorisaties, zoals de periodieke herbeoordeling van alle uitgegeven autorisaties en het naleven van de functiescheiding conform het bedrijfsbeleid.

Naast het inrichten van IAM voor interne medewerkers, kunnen ook derde partijen toegang krijgen tot interne informatie, diensten of faciliteiten. Dit soort gevallen worden in de basis op dezelfde manier beheerd (Koch & Möslein, 2005). Wel zijn de achterliggende technologieën die de processen ondersteunen vaak anders ten opzichte van die voor de interne medewerkers. Ook zijn hierbij vaak nog meer controles en maatregelen ingericht dan bij de interne organisatie.

Net als elk bedrijfsproces, wordt ook het IAM-proces steeds volwassener en robuuster naarmate de tijd vordert. Over het algemeen lijkt het erop dat organisaties in de financiële sector voorop lopen als het gaat om de IAM-volwassenheid ten opzichte van andere sectoren (Everett, 2011). Waarschijnlijk is dit door de hogere belangen die financiële instellingen hebben bij het minimaliseren van de risico's gerelateerd aan informatiebeveiliging. Het realiseren van een hoger volwassenheidsniveau wordt niet gekenmerkt door alleen maar het introduceren van nieuwe technologische oplossingen, maar juist door de IAM-organisatie en de controlerende processen steeds effectiever in te richten. Een voorbeeld hiervan is het steeds meer beleggen van verantwoordelijkheden bij de data-, systeem-, en proceseigenaren in plaats van dit volledig over te laten aan de IT-organisatie.

Uiteindelijk is het doel om een goede balans te vinden tussen een zo gebruiksvriendelijk mogelijke informatievoorziening en een zo robuust mogelijke informatiebeveiliging. IAM draagt hieraan bij door zich te richten op de processen die zowel ervoor zorgen dat individuen toegang krijgen tot de informatie, diensten en faciliteiten die ze nodig hebben voor hun werkzaamheden, maar ook te voorzien in inzicht en controle op alle uitgegeven autorisaties (Witty, Allan, Enck, & Wagner, 2003).

2.3.3 De veelvoorkomende beveiligingsincidenten veroorzaakt door insider threats

Bij beveiligingsincidenten veroorzaakt door insider threats wordt over het algemeen weinig gebruik gemaakt van geavanceerde technologie (Elifoglu, Abel, & Taşseven, 2018). Analytische software, complexe voorspellingsmodellen en technische oplossingen zoals antivirus, firewall en systemen die automatisch indringers detecteren bieden in dit opzicht weinig steun.

De beveiligingsincidenten die veroorzaakt worden door bewuste insider threats zijn divers van aard. Enkele opmerkelijke verhalen uit de media van de laatste jaren zijn onder andere:

- Een software engineer werkzaam bij Uber had duizenden bestanden over de technologie en algoritmes achter zelfrijdende auto's van zijn vorige werkgever gestolen en dit vervolgens met Uber gedeeld kort voordat hij daar in dienst ging (Lawler, 2017).
- Een medewerker van Ford had gepatenteerde documenten met vertrouwelijke informatie naar een externe harde schijf gekopieerd. Hij is vervolgens op het vliegveld gearresteerd nog net voordat hij zou vertrekken naar een nieuw baan bij een Chinese concurrent (FBI, 2011).
- Twee medewerkers die al voor langere tijd bij DuPont in dienst waren, hadden informatie gestolen over het ontwikkelproces van op titaandioxide gebaseerd verf (Wilber, 2016).
- Een voormalig medewerker van het bedrijf Fannie Mae had een zogeheten *logic bomb* geïnstalleerd. Indien die niet tijdig was ontdekt, had het potentieel duizenden servers met kritische bedrijfsinformatie vernietigd met alle gevolgen van dien (Moscaritolo, 2009).

Een afdeling van het Software Engineering Institute van de Carnegie Mellon University heeft in samenwerking met de U.S. Secret Service en de FBI een onderzoek (Miller, 2016) gedaan naar insider threats in de Verenigde Staten. Hieruit was gebleken dat de helft van de onderzochte organisaties tussen 2002 en 2014 elk jaar getroffen waren door een beveiligingsincident veroorzaakt door een insider threat. De meeste schade werd veroorzaakt in de vorm van:

- Diefstal van vertrouwelijke informatie (gepatenteerde informatie of bedrijfsgeheimen) (32%)
- Diefstal of oneigenlijk gebruik van klantgegevens (33%)
- Diefstal of oneigenlijk gebruik van medewerkersgegevens (40%)
- Het onbedoeld delen of publiceren van persoonsgegevens of vertrouwelijke informatie (50%)

In 2014 was een onderzoek (Cisco, 2014) gedaan naar datalekken als gevolg van het onbedoeld of onbewust delen of publiceren van vertrouwelijke informatie. Het onderzoek was uitgevoerd in 10 landen waarbij in elk land 100 eindgebruikers en 100 IT-professionals waren geïnterviewd. Wat in de meeste gevallen tot een datalek leidde was het ongeautoriseerd gebruikmaken van applicaties met gevoelige informatie (70%), anderen gebruik laten maken van persoonlijk apparatuur zonder zelf hier toezicht op te houden (44%), ongeautoriseerd gebruikmaken van informatie of faciliteiten (39%), het kopiëren van bedrijfsinformatie naar persoonlijke mediadragers zoals een USB-stick (46%) en het onderling delen van wachtwoorden met collega's (18%).

Bij beveiligingsincidenten veroorzaakt door bewuste acties is het altijd een combinatie van motief en kans dat tot actie leidt (Magklaras & Furnell, 2005). Bij incidenten ontstaan vanuit onbedoelde of onbewuste acties is de oorzaak in de meeste gevallen onwetendheid of onbekendheid met de gevaren die horen en consequenties die kunnen volgen door het (potentieel) onveilig gedrag.

2.3.4 De impact van veelvoorkomende beveiligingsincidenten veroorzaakt door insider threats

Uit de onderzoeken van de Carnegie Mellon University (Miller, 2016) en Cisco (2014), maar ook uit de opmerkelijke verhalen uit de media van de laatste jaren valt te concluderen dat de veelvoorkomende beveiligingsincidenten veroorzaakt door insider threats voornamelijk gerelateerd zijn aan datalekken en het oneigenlijk gebruik maken van vertrouwelijke informatie.

De impact van beveiligingsincidenten waarbij sprake is van datalekken of het oneigenlijk gebruik van vertrouwelijke informatie kan verschillen afhankelijk van de classificatie van de informatie. Eén van de aspecten van het goed inrichten van informatiebeveiliging is het aanbrengen van dataclassificaties (Tankard, 2015). Hoewel classificaties per organisatie kunnen verschillen, wordt het aangeraden om een classificatiemodel te hanteren die zowel voor de beveiligingsfunctionarissen als voor de overige medewerkers werkbaar en toepasbaar is. Afhankelijk van de classificatie toegekend aan informatie, kan de impact van incidenten betreffende de informatie snel worden bepaald en daarbij passende (preventieve) maatregelen worden ingericht.

Medewerkers met bewuste kwaadaardige bedoelingen gaan in veel gevallen voor informatie dat in het algemeen als middel tot zeer vertrouwelijke informatie geclassificeerd zou zijn (Huth, Chadwick, Claycomb, & You, 2013). Doordat deze personen vaak veel risico nemen, gaan ze vaak ook direct voor informatie waar veel kans is om een persoonlijk voordeel uit te halen. Het doel is dan vaak ook gepatenteerde informatie of bedrijfsgeheimen (Miller, 2016). Bij de gevallen waarbij onbewust vertrouwelijke informatie gelekt of verspreid wordt, verschilt de mate van gevoeligheid enorm. De meest ernstige gevallen hier zijn de gevallen waarbij sprake is van het lekken van persoonsgegevens.

Er zijn maar weinig methodes waarmee objectief berekend kan worden wat het financiële gevolg is van een organisatie getroffen door een datalek (Goel & Shawky, 2009). Het is immers lang niet altijd mogelijk om een direct verband te leggen tussen het beveiligingsincident en de financiële gevolgen voor de organisatie. Door wet- en regelgeving zijn organisaties verplicht om in sommige gevallen een datalek te melden. Zo ook in Nederland conform de Wet Meldplicht Datalekken die sinds 1 januari 2016 in werking is. Het verschilt per land wanneer een datalek gemeld moet worden. In Nederland moet een organisatie volgens de Wet Meldplicht Datalekken altijd een melding doen in het geval dat de (potentiele) impact van het incident betrekking heeft op de bescherming van persoonsgegevens of de persoonlijke levenssfeer van de betrokkenen (Custers, Dechesne, Georgieva, & Hof, 2017).

Een datalek heeft vaak gevolgen voor de publieke perceptie en het (potentiele) concurrentievoordeel van een organisatie. In sommige gevallen wordt ook een geldboete opgelegd door de toezichthouder (Kroeks-de, Westerdijk, & Zwenne, 2016). Organisaties getroffen door een datalek worden vaak na de bekendmaking voor lange tijd als onbetrouwbaar gezien. Dit leidt ertoe dat klanten zich anders gaan opstellen tegenover de organisatie (Curtis, Carre, & Jones, 2018). Soms kiezen organisaties ervoor om bewust een datalek niet te melden, echter staan hier ook geldboetes op. In Nederland betreft dit maximaal een geldbedrag van €820.000 of 10% van de jaaromzet (Verheij, 2016).

2.3.5 IAM-beveiligingsmaatregelen gericht op het verlagen van de kans op insider threats

De ISO27001 standaard is een wereldwijde erkende norm voor informatiebeveiliging (Calder, 2013). De standaard onderscheid vier categorieën voor het indelen van beveiligingsmaatregelen, namelijk preventief, detectief, repressief en correctief. Preventieve maatregelen zijn gericht op het verlagen van de kans op een beveiligingsincident. De meeste beveiligingsincidenten veroorzaakt door insider threats zijn het oneigenlijk gebruikmaken of het uitlekken van vertrouwelijke bedrijfsinformatie (Miller, 2016). Medewerkers horen bedrijfsinformatie altijd enkel en alleen te gebruiken voor het uitvoeren van hun dagelijkse werkzaamheden. Bij het gebruikmaken van bedrijfsinformatie op een ander moment of voor andere doeleinden is dus altijd sprake van het oneigenlijk gebruikmaken van informatie (Sandhu, Coyne, Feinstein, & Youman, 1996).

De overweging of verleiding om een misdrijf te plegen bestaat uit drie factoren. De hoeveelheid vereiste inspanning, de eventuele risico's (zoals de pakkans) en de verwachte opbrengsten. Dezelfde factoren gelden ook bij de overweging om bewust oneigenlijk gebruik te maken van vertrouwelijke informatie voor het eigen gewin (Padayachee, 2016). Maatregelen die deze factoren beïnvloeden kunnen dus ervoor zorgen dat de verleiding daalt. Identity & Access Management is gebaseerd op drie fundamentele aspecten die hierbij kunnen helpen. Dat zijn het toekennen en administreren van alle uitgegeven autorisaties, het rapporten over werkelijk uitgegeven autorisaties en het corrigeren van autorisaties aan de hand van rapportages en het autorisatiebeleid (Gunter et al., 2011). Het doel is om ervoor te zorgen dat medewerkers enkel en alleen geautoriseerd zijn tot de informatie die ze nodig hebben voor het kunnen uitvoeren van hun dagelijkse werkzaamheden.

Identity & Access Management voorziet in meerdere oplossingen en maatregelen om hier vorm aan te geven. Maatregelen die voorzien in het beperken van de toegang tot informatie zijn onder andere het proces voor het toekennen en herzien van autorisaties bij indiensttreding, interne verplaatsingen en uitdiensttreding, het scheiden van kritische taken en verantwoordelijkheden, het toekennen van autorisaties op basis van functieprofielen en de periodieke herbeoordeling van uitgegeven autorisaties (Witty et al., 2003). Samen kunnen deze maatregelen een positief effect hebben op het verlagen van de kans op (langdurig) ongeoorloofd toegang tot informatie.

In het geval dat een medewerker oneigenlijk gebruik maakt van bedrijfsinformatie waar hij of zij met legitieme redenen toegang tot heeft, dan biedt IAM weinig tot geen detectieve maatregelen om dit te detecteren (Fuchs & Pernul, 2012). Andere aandachtsgebieden binnen de informatiebeveiliging, zoals Security Information & Event Management (SIEM), kunnen vaak wel het gebruik van informatie direct inzichtelijk maken en analyseren op potentiele afwijkingen (Cappelli, Moore, & Trzeciak, 2012). Bijvoorbeeld als zeer vertrouwelijke informatie continu buiten kantoortijd of vanuit een externe locatie wordt geraadpleegd. IAM kan wel voorzien in het monitoren en beperken van het gebruik van *high privileged accounts*. Dit zijn speciale accounts, zoals beheerderaccounts en serviceaccounts die uitzonderlijk veel autorisaties hebben ten opzichte van persoonlijke accounts. Het zijn vaak ook de accounts waar veel informatie mee geraadpleegd kan worden en het soms ook mee mogelijk is om de logbestanden van deze acties te verwijderen (Lewis, 2012). Het beheren van dit soort accounts heet *Privileged Account Management* (PAM) (Dinoor, 2010). Met technische oplossingen is het zelfs mogelijk om het gebruik van dit soort accounts continu te monitoren en beperken. Voorbeelden hiervan zijn onder andere het genereren en uitgeven van tijdelijke wachtwoorden en het opnemen en registreren van alle acties gedaan met dit soort accounts.

Voor het verlagen van de kans op beveiligingsincidenten veroorzaakt door onbedoelde bedreigingen gelden dezelfde maatregelen als bij een bewuste bedreiging (Liu & Murphy, 2015). Echter, in het geval dat een medewerker per ongeluk vertrouwelijke informatie deelt of bedrijfsapparatuur met vertrouwelijke informatie kwijtraakt dan zijn andere correctieve maatregelen vereist die niet binnen het aandachtsgebied van IAM vallen. Dit zijn maatregelen zoals het toepassen van data encryptie en implementeren van technische oplossingen zoals Data Loss Prevention (Cappelli et al., 2012).

2.3.6 IAM-beveiligingsmaatregelen gericht op het verlagen van de impact door insider threats

De ISO27001 standaard, een wereldwijde erkende norm voor informatiebeveiliging (Calder, 2013), onderscheid vier categorieën voor het indelen van beveiligingsmaatregelen, namelijk preventief, detectief, repressief en correctief. Het verlagen van de impact van beveiligingsincidenten kan met een combinatie van detectieve en repressieve maatregelen. Waarbij detectieve maatregelen gericht zijn op het detecteren dat een incident heeft plaatsgevonden en de repressieve maatregelen gericht zijn op het beperken van de impact van een incident nadat deze heeft plaatsgevonden.

Binnen de informatiemanagement en daarmee ook de informatiebeveiliging is een bekend model de DIKW hiërarchie (Aven, 2013). De afkorting staat voor Data, Informatie, Kennis en Wijsheid. Binnen de hiërarchie is data een objectief waarneembaar feit. Informatie is data waar vervolgens betekenis en/of waarde aan is gegeven. Kennis is het weten hoe de informatie binnen een context gebruikt kan worden. Wijsheid is wanneer het duidelijk is waarvoor of waarom de informatie relevant is binnen de gegeven context. Met andere woorden, om oneigenlijk gebruik te kunnen maken van informatie, zal een bewuste bedreiging niet alleen toegang tot data en informatie moeten hebben, maar ook de kennis en wijsheid moeten hebben om te weten hoe en waarvoor het gebruikt kan worden.

De basisprincipes van Identity & Access Management zorgen al ervoor dat een medewerker niet op de hoogte hoeft te zijn van alle beschikbare informatie binnen de organisatie. Medewerkers horen immers alleen toegang te hebben tot de bedrijfsinformatie die relevant is voor het kunnen uitvoeren van hun dagelijkse werkzaamheden (Sandhu et al., 1996). Alleen al het implementeren van de meest basale IAM-processen en principes zoals *'need-to-know'* en *'least-privilege'* kunnen voor een positief effect zorgen. De principes 'need-to-know' en 'least-privilege' betekenen dat alleen het minimale aan autorisaties vereist voor het kunnen uitvoeren van de dagelijkse werkzaamheden uitgegeven wordt. Ook het toepassen van functiescheiding zodat meerdere medewerkers nodig zijn voor het uitvoeren van kritische en fraudegevoelige taken zorgt ervoor dat het moeilijker wordt om als individu van data en informatie naar kennis en wijsheid te gaan en hier vervolgens misbruik van te maken.

Ook het IAM-proces van herbeoordeling van alle uitgegeven autorisaties bij interne verplaatsingen kan ervoor zorgen *'autorisation creep'* wordt voorkomen (Witty et al., 2003). Dit is het ongewenst en onbedoeld uitbreiden van de autorisaties van een medewerker doordat de medewerker meerdere functies binnen de organisatie heeft vervuld. Een voorbeeld hiervan is een medewerker die voorheen de inkoop deed en nu bij de crediteurenadministratie werkt. Door de opstapeling van autorisaties, zou de medewerker nu geheel zelfstandig een inkoopopdracht kunnen invoeren en uitbetalen.

Echter, opnieuw kan het voorkomen dat een medewerker met legitieme redenen toegang heeft tot data of informatie. Ook in dit geval biedt IAM weinig tot geen repressieve maatregelen om de impact te beperken (Fuchs & Pernul, 2012). Voor dit soort gevallen zou data-abstractie mogelijk meer effect hebben. Een voorbeeld van data-abstractie is het inzichtelijk maken van NAW-gegevens van klanten, maar het afschermen van vertrouwelijke en/of fraudegevoelige informatie zoals het BSN-nummer. IAM biedt wel detectieve en repressieve maatregelen voor in het geval dat bijvoorbeeld sprake is van een onbewuste bedreiging. Geavanceerde maatregelen zoals *continuous authentication* kunnen ervoor zorgen dat een gebruiker continu wordt geauthentiseerd in plaats van alleen bij de initiële aanmelding (Clarke & Furnell, 2007). Zo kan bij diefstal van bedrijfsapparatuur bijvoorbeeld worden gedetecteerd dat het apparaat zich niet meer in een veilige omgeving bevindt en daar vervolgens automatisch en adequaat op worden gereageerd.

2.4 Doel van het vervolgonderzoek

De resultaten van het literatuuronderzoek duiden aan dat veelvoorkomende beveiligingsincidenten veroorzaakt door insider threats met name betrekking hebben op het oneigenlijk gebruikmaken of het uitlekken van (vertrouwelijke) bedrijfsinformatie. De beveiligingsincidenten zijn te onderverdelen in twee categorieën. Namelijk de bewuste gevallen en de onbewuste en/of onbedoelde gevallen. Bij de bewuste gevallen is het vaak een combinatie van motief en kans dat tot het ondernemen van een actie leidt. Bij de incidenten ontstaan vanuit onbedoelde of onbewuste acties, is de oorzaak vaker onwetendheid of onbekendheid met de gevaren en consequenties die verbonden zijn aan het (potentieel) onveilig gedrag.

Om de kans op en impact van beveiligingsincidenten te verlagen kunnen preventieve, detectieve, repressieve en correctieve maatregelen worden genomen. Het doel van IAM is om ervoor te zorgen dat medewerkers enkel en alleen geautoriseerd zijn tot de informatie die nodig is voor het kunnen uitvoeren van hun dagelijkse werkzaamheden. Preventieve maatregelen zoals het rapporteren over werkelijk uitgegeven autorisaties en het corrigeren van autorisaties aan de hand van de rapportages en het autorisatiebeleid kunnen hier een positieve bijdrage aan leveren. Het is juist in het geval dat als een medewerker met legitieme redenen toegang tot data of informatie heeft, dat de effectiviteit van de IAM-maatregelen aanzienlijk daalt. Zodoende is het aanbevolen om de maatregelen uit IAM zo veel mogelijk te combineren met maatregelen uit andere aandachtsgebieden of technologieën zoals data encryptie en Data Loss Prevention software.

Met de kennis opgedaan in het literatuuronderzoek kan het tweede deel van het onderzoek worden uitgevoerd, namelijk het empirisch onderzoek. De doelstelling van het empirisch onderzoek is om de argumenten en theorieën betreffend de effectiviteit van IAM-maatregelen, zoals deze gevonden zijn in het theoretisch kader, te toetsen aan de werkelijkheid. Organisaties nemen de dreiging die insider threats kunnen vormen steeds serieuzer en zien onder andere Identity & Access Management als een mogelijke oplossing om zich hiertegen te beschermen.

Om de theorie met de werkelijkheid te vergelijken worden beveiligingsincidenten uit het verleden met het theoretisch kader vergeleken. Relevante aspecten voor de vergelijking zijn onder andere de omstandigheden die tot het incident hebben geleid, de risico's die de medewerker heeft moeten nemen, de achterliggende motieven, hoe en wanneer het misbruik is gedetecteerd, wat de status van de informatiebeveiliging en IAM-organisatie destijds was, hoe tijdens het incident gehandeld is, of bepaalde IAM-maatregelen dit had kunnen voorkomen en wat voor maatregelen na afloop zijn genomen om de kans op en impact van een soortgelijk incident in de toekomst te beperken.

3. Methodologie

3.1 Conceptueel ontwerp: keuze van onderzoeksmethode(n)

Gezien de doelstelling om in het empirische onderzoek de gevonden theorie met de werkelijkheid te vergelijken, is een kwalitatieve onderzoeksmethode wenselijk. Een onderzoeksmethode die gericht is op het analyseren van gebeurtenissen uit de realiteit is de *case study*. Het is een onderzoeksmethode die in het bijzonder geschikt is om antwoord te geven op hoe en waarom vragen (Yin, 2014). Een case study kan enkelvoudig of meervoudig zijn opgezet. Bij een enkelvoudige case study wordt slechts één case onderzocht, bij een meervoudige case study zijn het twee of meer. Binnen een case study is de definitie van wat een case is, geheel afhankelijk van de context. Dit zou bijvoorbeeld een organisatie kunnen zijn, maar ook een persoon, voorwerp of type gebeurtenis. Daarnaast kan een case ook nog geanalyseerd worden als één geheel (*holistic*) of als afzonderlijke analyse-eenheden die samen het geheel opmaken (*embedded)*. Een voorbeeld van dit verschil is het beschouwen en analyseren van een organisatie als één geheel, of door juist de verschillende organisatieonderdelen te beschouwen en onderzoeken als afzonderlijke analyse-eenheden die samen het geheel vormen.

Voor het empirische deel van dit onderzoek is gekozen voor een meervoudige case study. Ondanks dat een enkelvoudige case study soms al voldoende resultaten kan leveren, zijn volgens Yin (2014) de resultaten van een meervoudige case study vaak robuuster en betrouwbaarder. Het nadeel van een meervoudige case study is dat het, ten opzichte van een enkelvoudige case study, altijd meer tijd en moeite kost. Zodoende is met inachtneming van de beschikbare tijd voor het onderzoek besloten om elke case als één geheel te beschouwen en onderzoeken. Kortom, het onderzoek wordt uitgevoerd in de vorm van een meervoudige holistische case study.

Tot nu toe heeft het onderzoek zich gericht op zowel de bewuste als de onbewuste en onbedoelde beveiligingsincidenten veroorzaakt door insider threats. Echter, voor het empirische gedeelte van het onderzoek is gekozen om een case te definiëren als het voordoen van een beveiligingsincident door een **bewuste** insider threat. De reden voor deze beslissing is vanwege dat alle cases een soortgelijk karakter moeten hebben om ze onderling met elkaar te kunnen vergelijken, zoals in dit geval het hebben van een bewust motief. De keuze om het empirisch onderzoek uitsluitend te richten op de bewuste dreigingen, is vanwege dat bij bewuste dreigingen vaak meer achter het ontstaan van het incident zit. Vragen betreffende de motivatie, het doel, de genomen risico's en de mogelijkheden waardoor het incident kon ontstaan zijn immers niet altijd of op dezelfde wijze van toepassing bij de onbewuste of onbedoelde gevallen.

3.2 Technisch ontwerp: uitwerking van de methode

In lijn met de opzet voor een meervoudige case study, worden drie cases gekozen waarbij sprake is van een bewuste insider threat die zich manifesteerde of dreigde te manifesteren tot een incident. De criteria voor de te selecteren cases is afhankelijk van een aantal variabelen. Voor het onderzoek is gekozen om alle cases te beperken tot gebeurtenissen in de financiële sector. De incidenten moeten in de laatste 5 jaar zijn voorgekomen en de dreiging moet altijd precies één medewerker betreffen. Kortom, incidenten waarbij meerdere personen in samenwerking handelden zijn uitgesloten. Verder moeten alle cases betrekking hebben op het oneigenlijk gebruikmaken of het uitlekken van (vertrouwelijke) bedrijfsinformatie.

Van elke case moet vastgesteld worden (1) wat was de aard van het (potentiële) incident, (2) op welke wijze is misbruik gemaakt van (vertrouwelijk) bedrijfsinformatie, (3) met welk doel handelde de medewerker, (4) wat voor risico's heeft de medewerker genomen, (5) hoe en wanneer is het incident gedetecteerd, (6) wat voor IAM-maatregelen waren destijds ingericht, (7) wat voor maatregelen zijn na de evaluatie van het incident genomen en (8) wat voor IAM-maatregelen hadden dit incident kunnen voorkomen?

Om een antwoord te krijgen op deze vragen is een combinatie van interviews en documentanalyse gewenst. Om inzicht in de aard van het incident te krijgen worden de medewerkers verantwoordelijk voor de informatiebeveiliging geïnterviewd omtrent de aard van het incident en de inrichting van informatiebeveiliging ten tijde van het incident. In het bijzonder wordt ingegaan over de destijds geïmplementeerde IAM-maatregelen. Vanzelfsprekend zal de betrokken medewerker niet langer in dienst zijn, zodoende wordt de leidinggevende en een directe collega van de medewerker geïnterviewd om inzicht te krijgen in de werkbeleving en het functioneren van de medewerker.

Een aanname en uitgangspunt is dat alle incidenten geadministreerd zijn met alle aan het incident gerelateerde documentatie. Het verzoek zal zijn om inzicht te krijgen in deze documenten om te onderzoeken hoe het incident zich in eerste instantie heeft kunnen voordoen, wanneer en hoe het incident is gedetecteerd en wat voor maatregelen na afloop zijn ingericht. Hierbij bestaat de mogelijkheid dat directe inzage niet is toegestaan. Daarvoor kan als alternatief een interview met een medewerker van de afdeling veiligheidszaken uitkomst bieden.

Alle interviews vinden plaats op het kantoor van de standplaats van de respondent. Vooraf aan het afnemen van de interviews wordt een lijst met onderwerpen en vragen opgesteld bedoeld om het interview te sturen, maar niet te beperken. De respondenten worden vooraf ingelicht over de onderwerpen die ter sprake komen, maar krijgen geen inzage in de volledige vragenlijst om te voorkomen dat ze vooraf aan het interview al mogelijk wenselijk antwoorden bedenken. Uiteindelijk is het doel om meerdere semigestructureerde diepte-interviews af te nemen waardoor de resultaten over de verschillende cases heen vergelijkbaar zouden moeten zijn.

3.3 Gegevensanalyse

De intentie van de gegevensanalyse is om de complexe en soms abstracte resultaten te vertalen naar meetbare termen. Voor het analyseren van de resultaten uit de interviews wordt gebruikt gemaakt van de *Codes en Coding*-techniek (Miles & Huberman, 1994) die versimpeld en verduidelijkt is door Atkinson (2002). Het idee achter de techniek is om fragmenten uit de interviews te coderen. Coderen kan ook worden gezien als het categoriseren of labelen van informatie. Dit met de intentie om het herkenbaar te maken en te relateren aan een bepaald onderwerp of thema binnen het onderzoek.

Een belangrijk onderdeel van het proces is het opstellen van de codes. Het is essentieel dat ze alle relevante onderwerpen en thema's omvatten, maar niet overlappen of gelijkenissen vertonen om te voorkomen dat ze lastig te onderscheiden zijn. Het groeperingsprincipe MECE, een Engelse afkorting voor de term *Mutually Exclusive, Collectively Exhaustive* (Raisel, 1998), is bij uitstek hiervoor geschikt. Dit principe is gebaseerd op de gedachte dat alle codes qua betekenis of interpretatie onderling niet mogen overlappen, maar gezamenlijk wel, voor zover mogelijk, alle opties representeren. Op basis van de codes worden de afzonderlijke interviews gecodeerd. Tijdens het coderen komt het geregeld voor dat codes worden toegevoegd, samengevoegd of zelfs in het geheel worden verwijderd. De analyse zelf wordt gedaan door de uiteindelijke resultaten gegroepeerd per code te analyseren en daar een conclusie uit te trekken.

Ondanks dat het afnemen van interviews en het coderen hiervan een veelgebruikte techniek is bij een kwalitatief onderzoek, heeft het zoals elke ander methode ook nadelen. Zo kan het bijvoorbeeld voorkomen dat de interviewer het interview te veel stuurt waardoor de respondent alleen de gewenste antwoorden geeft in plaats van vrijuit te spreken. Ook beslist de interviewer vaak zelf wie geïnterviewd wordt (Alsaawi, 2014). Voor wat het coderen betreft, zijn de codes vaak ook zelfstandig door de interviewer opgesteld en dus beïnvloed door hoe de interviewer ze interpreteert (Campbell, Quincy, Osserman, & Pedersen, 2013). Zo wordt ook dit onderzoek door één onderzoeker uitgevoerd en is het dus belangrijk om zo veel mogelijk vooroordelen te voorkomen. Dit kan bijvoorbeeld door de antwoorden na afloop door de respondent te laten controleren om te voorkomen dat eigen interpretaties van de gegeven antwoorden verwerkt worden als feitelijke waarnemingen.

De techniek die gebruikt wordt voor het coderen van interviews kan ook worden gebruikt voor het analyseren van documenten. Hierbij is immers ook sprake van fragmenten kwalitatieve informatie die geanalyseerd moeten worden (Elo & Kyngäs, 2008). In dit onderzoek wordt dan ook dezelfde techniek als bij de interviews gebruikt waarbij meerdere codes worden opgesteld die gekoppeld worden aan de tekstfragmenten uit de geanalyseerde documenten. Uiteraard zijn de nadelen van de techniek, net als bij het afnemen van interviews, ook bij het analyseren van documenten van toepassing. Het borgen van de betrouwbaarheid en validiteit zijn dan ook cruciale aspecten van de dataverzameling en gegevensanalyse.

3.4 Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

Het is van groot belang dat het onderzoek wordt uitgevoerd op een wijze die valide en betrouwbaar is. Een onderzoek is valide wanneer hetgeen wat beoogd was om te meten ook werkelijk hetgeen is wat binnen het onderzoek gemeten wordt. De betrouwbaarheid gaat juist over de mate waarin het onderzoek te herhalen is en dan tot dezelfde resultaten leidt. Yin (2014) specificeert vier criteria die belangrijk zijn voor het bepalen of een onderzoek valide en betrouwbaar is. Dat zijn begripsvaliditeit, interne validiteit, externe validiteit en betrouwbaarheid (reproduceerbaarheid). Daarnaast kunnen ook de ethische aspecten van het onderzoek een rol spelen.

Begripsvaliditeit

De definitie van begripsvaliditeit is dat het onderzoek gericht is op het meten wat beoogd was om te meten. Zo zijn bepaalde begrippen simpelweg makkelijker te meten dan anderen. Een voorbeeld van een begrip dat lastig te meten is, is het begrip effectiviteit. Om de begripsvaliditeit in dit onderzoek te borgen worden vragen aangaande specifieke onderwerpen niet uitgevraagd in een vraagstelling zoals ‘wat vindt u van de informatiebeveiliging?’. In plaats daarvan worden over alle onderwerpen vragen gesteld over de feitelijke aspecten van het onderwerp, zoals bijvoorbeeld ‘op welke wijze kunnen beveiligingsincidenten worden gemeld?’. Dit om meningen en feiten zo veel mogelijk van elkaar te kunnen onderscheiden. Uiteraard blijft dit moeilijk vanwege dat een mate van eigen interpretatie door de respondent die zich altijd blijft voordoen.

Interne validiteit
De interne validiteit gaat over het onderzoeken van het onderwerp wat daadwerkelijk ook beoogd was om te onderzoeken. Een onderzoek is intern valide wanneer de gebruikte onderzoekmethodes geleid hebben tot een situatie waarbij op de juiste wijze conclusies getrokken zijn. Kortom, het systeem dat tot de resultaten heeft geleid moet in de basis deugdelijk zijn. In dit onderzoek is dit gerealiseerd door de onderzoeksmethode te baseren op academische bronnen en methodieken. Ook is vooraf aangeduid op welke wijze de informatie verzameld en geanalyseerd wordt, evenals hoe de uiteindelijke conclusies getrokken worden. Bij een kwalitatief onderzoek speelt daarnaast ook mee dat de onderzoeker in staat is om de interviews zodanig te beïnvloeden dat een vertekend beeld kan ontstaan. Om dit te voorkomen wordt na afloop van elk interview een uitwerking opgesteld en gedeeld met de respondent zodat, indien gewenst, de respondent kan verifiëren dat de uitwerking overeenkomt met de bedoelde uitingen. Deze methode heet ook wel een *membercheck*.

Externe validiteit
De externe validiteit betreft de mate van generaliseerbaarheid van het onderzoek in bijvoorbeeld andere sectoren, situaties of gevallen dan die behandeld in het onderzoek. Het generaliseren van een kwalitatief onderzoek kan soms minder van belang zijn dan bij een kwantitatief onderzoek. Echter, het doel van dit onderzoek is om te toetsen of de theorie overeenkomt met de werkelijkheid. Met dat als uitgangspunt was ook besloten om meerdere cases te onderzoeken. Ondanks dat de cases zelf beperkt worden tot de financiële sector, is het theoretisch kader dat niet. In praktijk is de generaliseerbaarheid van het empirische onderzoek beperkt tot de financiële sector totdat het onderzoek ook in andere sectoren is herhaald.

Betrouwbaarheid
De betrouwbaarheid van het onderzoek gaat over de mate waarop het onderzoek reproduceerbaar is. Het doel hiervan is dat als het onderzoek herhaald zou worden onder dezelfde omstandigheden, dat het opnieuw tot dezelfde resultaten zou leiden. Dit kan bijvoorbeeld door hetzelfde onderzoek meerdere keren uit te voeren. Echter, door de beperkte middelen en tijd is dit geen optie binnen dit onderzoek. Als alternatief hiervoor wordt een logboek bijgehouden van de acties, gebeurtenissen en omstandigheden waarin het onderzoek is uitgevoerd (audit trail). Hiermee kunnen anderen inzicht krijgen in de wijze waarop de onderzoeksgegevens zijn verzameld en verwerkt. Dit zorgt ervoor dat het onderzoek niet alleen herhaalbaar zou zijn met dezelfde gegevens, maar ook navolgbaar.

Ethische aspecten
De ethische aspecten gaan over het garanderen van onafhankelijkheid, onpartijdigheid, privacy en veiligheid van de respondenten en de gebruikte informatie in het onderzoek. Om onafhankelijkheid te garanderen worden de interviews alleen afgenomen met respondenten waar de onderzoeker geen hiërarchische of functionele relatie mee heeft. Om ervoor te zorgen dat de resultaten van het onderzoek onpartijdig zijn en de privacy van de respondenten te waarborgen, worden de betrokken organisaties en respondenten nergens in het onderzoek bij naam genoemd. Dit onderzoek moet ook geen invloed hebben op (de perceptie van) het imago of de reputatie van de betrokken organisaties en personen. Als laatste wordt van elke respondent vooraf gevraagd of ze akkoord zijn met het afnemen van het interview en de wijze waarop de resultaten verwerkt worden.

4. Resultaten

4.1 Uitvoering gegevensverzameling

Het verzamelen van de gegevens voor het empirische onderzoek is het resultaat van het afnemen van interviews. De gegevensverzameling is bij alle cases op dezelfde wijze uitgevoerd.

Benaderen respondenten

De organisaties en respondenten gebruikt voor dit onderzoek komen vanuit het eigen netwerk van de onderzoeker of zijn aanbevolen door iemand uit het netwerk van de onderzoeker. Hierdoor is met elke respondent eerst telefonisch contact geweest. Met de onderzochte organisaties is afgesproken dat, vanwege het karakter van dit onderzoek, alle informatie dat in het kader van dit onderzoek verstrekt wordt als zeer vertrouwelijk moet worden behandeld. Zodoende worden de organisaties en respondenten in dit onderzoek niet bij naam genoemd en incidenteel alleen aangeduid met een alfanumerieke indicatie. Uiteindelijk is wel een vertrouwelijke bijlage opgesteld met de namen van de onderzochte organisaties en respondenten. Echter, deze bijlage is alleen inzichtelijk voor de examinatoren van de Open Universiteit en is in verband met de vertrouwelijkheid hiervan ook niet openbaar gepubliceerd.

Afname van interviews

In eerste instantie was het de bedoeling om van elke organisatie een functionaris verantwoordelijk voor de informatiebeveiliging en de voormalige leidinggevende en/of directe collega's van de dader te interviewen. Uiteindelijk was het helaas niet mogelijk om de voormalige leidinggevende en/of een collega van de dader te interviewen. Hierdoor is de lijst met interviewvragen aangepast om tijdens het interview met de functionaris verantwoordelijk voor de informatiebeveiliging hopelijk voldoende inzicht te krijgen in de relatie tussen de dader en zijn voormalige leidinggevende en collega's. De lijst met de vooraf opgestelde interviewvragen is in de bijlage opgenomen.

Methodiek voor transcriberen

Van alle interviews zijn, met toestemming van de respondenten, audio-opnames gemaakt. Vanwege de eis om alle verstrekte informatie als strikt vertrouwelijk te behandelen, zijn de audio-opnames alleen gebruikt voor het transcriberen van de gesproken tekst. De interviews zijn allemaal woordelijk uitgewerkt. Nadat het transcriberen was voltooid, zijn de audio-opnames direct vernietigd en zijn de respondenten hiervan op de hoogte gesteld. De interviewtranscripties zijn enkel op verzoek en met uiterst goede redenen bij de onderzoeker te verkrijgen.

Analyseren van verstrekte documenten

Initieel was het de bedoeling om de documenten relevant aan de cases op te vragen en te analyseren met als doel om daarmee een uitgebreider beeld van de cases te krijgen. Helaas was het bij geen enkele case toegestaan om inzicht in dit soort documenten te krijgen. Zodoende is deze analyse dan ook niet uitgevoerd.

4.2 Uitvoering gegevensanalyse

De analyse van de interviews is het resultaat van het transcriberen en vervolgens coderen van de uitwerkingen die door de respondenten, indien gewenst, zijn goedgekeurd. Het coderen gebeurt in drie fases: open, axiaal en selectief coderen. Deze fases hoeven niet noodzakelijk lineair te worden opgevolgd. Het kan en zal hierbij voorkomen dat een stap terug naar een vorige fase wordt gedaan op basis van nieuwe bevindingen. Het coderingsproces is bij alle cases op dezelfde wijze uitgevoerd.

Opstellen van codelijst met thema's (open coderen)

Voorafgaand aan het afnemen van de interviews is een codelijst opgesteld met de verwachte labels (codes) voor de tekstfragmenten uit de interviewtranscripties. De uitwerking van de codelijst is in de bijlage opgenomen. Open coderen is het simpelweg initieel labelen (coderen) van tekstfragmenten op basis van specifieke thema's. Hierdoor wordt eerst duidelijk wat het thema van het fragment betreft. Een voorbeeld van het open coderen is het labelen met het thema 'motief'.

Vergelijken, samenvoegen en splitsen van thema's (axiaal coderen)

Vervolgens wordt bij axiaal coderen de al toegewezen codes onderling met elkaar vergeleken om codes die bij elkaar horen, waar mogelijk, samen te voegen onder een overkoepelende code. In de realiteit kan het zijn dat een tekstfragment bij meerdere overkoepelende codes hoort. Dit leidt dan tot het ontstaan van hoofd- en subthema's. Bij axiaal coderen worden de interviewtranscripties ook allemaal onderling met elkaar vergeleken. Dit om ervoor te zorgen dat ze dezelfde overkoepelende codes hanteren voor de hoofd- en subthema's. Een voorbeeld van axiaal coderen is het labelen met het hoofdthema 'motief' aangevuld met het subthema 'wraak'.

Groeperen van resultaten per thema (selectief coderen)

Als laatste worden de tekstfragmenten selectief gecodeerd, dit draagt bij aan het verbanden leggen tussen concepten die vaker terugkomen om dit vervolgens te kunnen verwerken tot een theorie. De tekstfragmenten die dezelfde selectieve code delen kunnen ook gebruikt worden voor het vastleggen van de resultaten op een bepaalde thema en dienen als de basis voor de uiteindelijke conclusies. Een voorbeeld van selectief coderen is het uniformeren van alle tekstfragmenten met het subthema 'wraak' onder de selectieve code 'negatieve gevoelens'.

4.3 Omschrijving per case study

Hieronder worden de cases afzonderlijk van elkaar omschreven. Dit om eerst per case een overzicht te hebben van de context rondom het incident en de wijze waarop alle informatie is verzameld.

4.3.1 Case study 1: Voor miljoenen euro's verduisteren dat bestemd was voor nabestaanden

Dit incident speelde zich af bij een grote Nederlandse vermogensbeheerder. De organisatie heeft in Nederland tussen de 500 en 1000 medewerkers, maar opereert ook wereldwijd met lokale kantoren in diverse landen. De organisatie heeft een volwassen informatievoorziening en heeft vanwege de diensten die ze aanbieden, informatiebeveiliging hoog op de agenda staan. Bij deze organisatie was een incident voorgekomen met een medewerker verantwoordelijk voor het afhandelen van een specifieke soort speciale transacties. Bij het afhandelen van de financiële transacties bestemd voor de nabestaanden van rekeninghouders, sluisde deze medewerker steeds een deel van het vermogen door naar andere bankrekeningen en verduisterde zo miljoenen euro's.

De informatie verzameld met betrekking tot dit incident is het resultaat van een interview met een medewerker werkzaam binnen het team dat verantwoordelijk is voor het dagelijkse beheer en onderhoud op alle informatiesystemen in gebruik door de ondersteunden afdelingen. De respondent werkt net iets minder dan 20 jaar bij de organisatie en heeft in die tijd verschillende functies vervuld. Ondanks dat de respondent geen functionaris informatiebeveiliging is, werkt de respondent wel zeer nauw samen met de afdeling informatiebeveiliging en vervuld hierbij vooral een adviserende rol.

4.3.2 Case study 2: Wraak nemen door opzettelijk bedrijfskritische informatie te verwijderen

De organisatie getroffen door dit incident is een grote Nederlandse financiële dienstverlener. In Nederland heeft de organisatie meer dan 1000 medewerkers. De organisatie heeft naar eigen zeggen een uitgebreid aanbod aan financiële diensten en producten. Informatiebeveiliging is voor de organisatie een belangrijk en integraal onderdeel van de bedrijfsvoering. Echter, ook zij zijn wel eens het slachtoffer van een incident. Net als toen een boze stagiair, na een felle woordenwisseling met zijn directe leidinggevende, op wraak uit was en besloot om opzettelijk kritische bedrijfsinformatie te verwijderen nog kort voordat hij het pand moest verlaten.

De resultaten van deze case study zijn het gevolg van twee aparte interviews. De eerste respondent is een medewerker fraudezaken die inhoudelijk de details van het incident heeft toegelicht. De tweede respondent is een functionaris informatiebeveiliging en heeft een uitgebreid verteld over de (destijds) ingerichte beveiligingsmaatregelen. De respondenten zijn beiden al meer dan 5 jaar bij de organisatie in vaste dienst.

4.3.3 Case study 3: Klanten misleiden en oplichten tot fraudeleuze overboekingen

Incidenten komen regelmatig voor en dan ook in allerlei soorten en maten. Dit incident deed zich bij dezelfde financiële dienstverlener voor als bij case study 2. Ditmaal had de organisatie te maken met een klantenservicemedewerker die klanten met opzet misleidde om ze betalingen voor openstaande facturen te laten overboeken naar zijn persoonlijke bankrekening.

De respondent die over dit incident heeft verteld was een andere medewerker die ook werkzaam is op de afdeling fraudezaken. Gedurende het interview is alleen het incident besproken en is de inrichting van de informatiebeveiliging achterwege gebleven. De functionaris informatiebeveiliging had bij de vorige case study al voldoende toegelicht over de beveiligingsmaatregelen die destijds waren ingericht en is zodoende niet opnieuw bevraagd met vragen specifiek betreffende dit incident.

4.4 Resultaten per thema

Hieronder volgen de resultaten van elke case study, gegroepeerd per thema. Door het groeperen is het direct mogelijk om de verschillen en gelijkenissen tussen de incidenten onderling te vergelijken.

4.4.1 Situatie: wat was de aard van het incident en hoe was het incident mogelijk gemaakt?

De eerste case wordt gekenmerkt door een vaste medewerker die al jaren in dienst was en in die tijd miljoenen euro's heeft verduisterd. Hij deed dit door bij de transacties die bestemd waren voor de nabestaanden een deel hiervan naar zichzelf over te boeken. Dit is jaren onopgemerkt gebleven vanwege dat dit soort transacties als uitzonderlijk werden beschouwd en niet onderhevig waren aan dezelfde controles als die binnen de rest van de organisatie. In de tweede case had een stagiair van de IT-afdeling met opzet kritische bedrijfsinformatie verwijderd. Dit gebeurde net na een kennelijke felle woordenwisseling met zijn leidinggevende. Volgens de respondent was de stagiair als gevolg daarvan waarschijnlijk dermate gefrustreerd dat hij dacht om op deze wijze wraak te nemen. Bij de derde case was sprake van een dader die op de klantenservice werkte en klanten misleidde. Geheel bewust communiceerde hij zijn eigen persoonlijke bankrekeningnummer naar klanten als die vroegen naar welk bankrekeningnummer ze de betaling van hun openstaande factuur moesten overmaken. Uiteindelijk heeft hij hiermee voor een klein geldbedrag kunnen frauderen voordat het werd opgemerkt. Hoewel de aard van de onderzochte incidenten van elkaar verschillen, hebben de daders in elk incident hun huidige positie en/of functie met de daarbij komende bevoegdheden weten te benutten om het incident te initiëren.

4.4.2 Motivatie: met welk doel handelde de dader en welke risico's zijn daarbij genomen?

Het motief waarmee de dader heeft gehandeld verschilt per case. In de eerste case, het verduisteren van miljoenen euro's bestemd voor nabestaanden, en derde case, het misleiden van klanten tot het overboeken van betalingen naar een persoonlijke bankrekening, was het motief financieel van aard. Bij de eerste case zou aanzien ook mogelijk een rol kunnen hebben gespeeld. De respondent gaf aan dat de dader steeds vaker dure en luxe artikelen ging aanschaffen om vervolgens hiermee op de afdeling te pronken. Bij de tweede case was wraak het motief. De dader wilde opzettelijk schade aanrichten als gevolg van de gebeurtenissen die daaraan vooraf gingen. Volgens de respondent van dit incident was dit waarschijnlijk door het gevoel van onrecht bij de dader. De respondent vermoed dat de relatief jonge leeftijd van de dader een rol heeft gespeeld door niet eerst volledig de consequenties van de wraakactie te overwegen.

4.4.3 Impact: wat voor consequenties had het incident voor de organisatie en de dader?

De eerste case, het verduisteren van geld, ging gepaard met een financiële impact van de 10 tot 15 miljoen euro dat was verduisterd. In de tweede case was vooral sprake van niet-financiële schade. Door het verwijderen van kritische en operationele bedrijfsinformatie, had de dader ervoor gezorgd dat de organisatie gedurende een periode niet in staat was om haar klanten optimaal te bedienen. In de derde case had de dader voor nog geen 2000 euro bij elkaar gefraudeerd. De respondent gaf aan dat de impact hierdoor voor de organisatie uiteindelijk vrij beperkt was. In geen enkele van de drie gevallen was iets naar de pers of een toezichthouder gecommuniceerd waardoor de cases geen impact hebben gehad op (de perceptie van) het imago van de betrokken organisaties.

De consequenties voor de daders lopen uiteen. Van de eerste en derde cases werd aangifte gedaan. In het geval van het verduisteren, werd een strafrechtelijke procedure tegen de dader begonnen dat eindigde in gevangenisstraf. Ook werd de dader verbannen van het werken in de financiële sector. De tweede case waarbij het een stagiair betreft, werd onderling afgedaan tijdens een gesprek met een vertegenwoordiger van zijn onderwijsinstelling. De dader van de derde case, het misleidden van klanten, werd per direct ontslagen. De organisatie deed daarnaast aangifte en een melding van fraude. De dader werd verbannen van het werken in de financiële sector en uiteindelijk is ook een strafrechtelijke procedure tegen hem gestart. De afloop daarvan was bij de respondent niet bekend.

4.4.4 Detectie: hoe en wanneer is het incident gedetecteerd?

De eerste case was al jaren gaande voordat het werd gedetecteerd. Het was volgens de respondent nooit eerder gedetecteerd vanwege dat de speciale transacties nauwelijks werden gecontroleerd. Preventieve maatregelen zoals het vierogenprincipe en functiescheiding waren voor alle afdelingen die de transacties afhandelde ingericht. Echter, speciale transacties waren, tot het voordoen van dit incident, daar nooit aan onderhevig. Medewerkers van de afdeling speciale transacties waren dus in staat om transacties geheel zelf in te voeren en goedkeuren. Of dit veranderde vanwege een klacht of vanwege een verbetering van de organisatie inrichting is niet duidelijk. De respondent gaf aan dat als de controles eerder waren geïmplementeerd, het incident dan ook zeer waarschijnlijk eerder was ontdekt. Dit is in contrast tot de tweede case, waarbij de impact vrijwel direct te merken was. De medewerkers van de klantenservice die afhankelijk waren van de verwijderde data hadden vrijwel direct een incident gemeld waarna de IT-dienstverlener van de organisatie dezelfde dag nog de oorzaak had achterhaald. Hetzelfde menselijke aspect was ook bij de derde case van toepassing. Meerdere klanten meldde dat ze een herinnering kregen van een openstaande factuur die ze naar eigen zeggen al eerder hadden betaald. Een collega van de dader ging de zaak onderzoeken voordat het formeel als potentiële fraude werd gemeld. In twee van de drie cases werd het incident pas na een melding door een persoon ontdekt. In alle gevallen hadden de organisaties naar eigen zeggen wel beveiligingsmaatregelen ingericht, maar waren die niet bedoeld om dit soort incidenten te voorkomen of zoals in het geval van de eerste case, niet van toepassing op de betrokken afdeling.

4.4.5 Repressie: welke maatregelen hebben bijgedragen aan het beperken van de schade?

In de eerste en tweede case hadden de betrokken organisaties geen repressieve maatregelen ingericht die hadden bijgedragen aan het beperken van de opgelopen schade. In de eerste case was de afdeling jarenlang buiten het gezichtsveld gebleven van de meeste controles en maatregelen en kon de dader hierdoor ongestoord zijn daad verrichten. Een maatregel die, volgens de respondent, in de derde case eventueel had kunnen bijdragen aan het beperken van de schade, was het toepassen van het vierogenprincipe op alle uitgaande communicatie. Hierbij gaf de respondent wel aan dat dit in de praktijk zeer waarschijnlijk te omslachtig zou zijn om daadwerkelijk te kunnen implementeren. In de tweede case had de dader zonder moeite data kunnen verwijderen en hierdoor de opgelopen schade kunnen verrichten. De functionaris informatiebeveiliging reageerde hierop door aan te geven dat de organisatie tot op heden geen maatregelen heeft genomen om dit soort acties te weren. Anderzijds, de organisatie heeft wel maatregelen ingericht om (eventueel per ongeluk) verwijderde data snel te kunnen herstellen en op deze wijze de continuïteit van de organisatie te waarborgen.

4.4.6 Correctie: wat voor correctieve en preventieve maatregelen zijn na afloop genomen?

Bij de eerste case had het incident een dermate hoge impact voor de organisatie, dat een speciaal team in het geheim werd opgericht om oplossingen te bedenken en implementeren om de kans op een soortgelijk incident in de toekomst te voorkomen. Het idee was om te komen tot betere en frequentere controle op alle financiële transacties. Ook werden alle controles die in de rest van het bedrijf van toepassing waren, ook op de afdeling waar het incident had plaatsgevonden toegepast. In het geval van de tweede case werd de actie door de functionaris informatiebeveiliging vergeleken met het per ongeluk verwijderen van kritische en/of operationele data. Voor dat soort gevallen had de organisatie al bestaande corrigerende maatregelen om (per ongeluk) verwijderde data snel te kunnen herstellen. Hierdoor zijn na afloop van het incident geen nieuwe maatregelen getroffen. In de derde case ging het om de communicatie tussen de organisatie en haar klanten. De respondent gaf aan dat geautomatiseerde data-analyses op alle communicatie een mogelijke optie zou kunnen zijn om voortaan preventief te kunnen handelen. Echter, concrete maatregelen zijn vooralsnog niet genomen en de organisatie heeft ook nog geen plannen om dit soort maatregelen in de toekomst te gaan implementeren.

5. Discussie, conclusies en aanbevelingen

5.1 Discussie - reflectie

Onderdeel van de discussie is het specifiek reflecteren op de betrouwbaarheid, validiteit en ethische aspecten van het onderzoek. De reflectie op deze aspecten is hieronder verder toegelicht.

Betrouwbaarheid

Verschillende maatregelen hebben bijgedragen aan het zo mogelijk betrouwbaar maken van de resultaten. Voor het afnemen van de interviews is een semigestructureerde aanpak gehanteerd. Alle respondenten zijn dezelfde vragen gesteld in dezelfde volgorde. Ook hebben alle respondenten vooraf dezelfde contextinformatie over het doel van het interview gekregen. De te meten begrippen zijn vooraf uitgelegd zodat iedereen de definities begrijpt en op dezelfde wijze hanteert. Voor het coderen van de interviewtranscripties is gebruik gemaakt van software die het coderingsproces vergemakkelijkt en overzichtelijk maakt. Het coderingsproces en de gebruikte codes zijn bij alle interviewtranscripties op dezelfde wijze toegepast conform het coderingsprotocol. Minder sterk is de triangulatie van de resultaten. Initieel was het de bedoeling om documentanalyse te doen en de voormalige leidinggevende en/of directe collega's van de dader te spreken. Beiden waren niet mogelijk waardoor de resultaten beperkt zijn tot het perspectief van de respondent. Ook waren de respondenten niet altijd op hetzelfde niveau qua kennis en ervaring met informatiebeveiliging. Bij de één van de organisaties zijn de gesprekken dan ook opgesplitst tussen de medewerkers fraudezaken en een functionaris informatiebeveiliging om zo tot een compleet beeld van de situatie te komen.

Validiteit

Het doel was om van elke case een verdiepend gesprek te hebben over de verschillende aspecten. De semigestructureerde aanpak heeft hier een positief effect op gehad. Wel valt op te merken dat de respondenten niet in alle gevallen alle perspectieven goed konden belichten. Het zou krachtiger zijn geweest als meerdere respondenten vanuit verschillende perspectieven toelichting hadden gegeven. Dit zou tot een ander en/of uitgebreider beeld kunnen hebben geleid over bijvoorbeeld de motivatie van de verdachte. De documentanalyse was initieel bedoeld om de interviews te ondersteunen met de gerapporteerde waarnemingen vanuit de organisatie. Helaas was het niet toegestaan om dit soort documenten in te zien waardoor deze vorm van triangulatie niet mogelijk was. Dit had de validiteit verder kunnen versterken. Verder is de generaliseerbaarheid van de resultaten beperkt. Uiteindelijk zijn slechts drie cases onderzocht van de potentieel duizenden incidenten die zich in de afgelopen jaren hebben voorgedaan. Ook waren de cases qua motivatie en impact niet van hetzelfde niveau waardoor onderlinge vergelijking niet altijd even krachtig was.

Ethische aspecten

De ethische aspecten gaan over de onafhankelijkheid, onpartijdigheid, privacy en veiligheid van de respondenten en de verzamelde informatie. De respondenten zijn vooraf aan de interviews allemaal ingelicht over de aard van het onderzoek, wat voor informatie getracht wordt te verzamelen en waar de verstrekte informatie voor gebruikt zou worden. In geen enkel geval is een respondent verplicht om mee te doen en/of gevraagd om informatie te verstrekken die ze eigenlijk niet wilde verstrekken. In tegenstelling tot de initiële verwachting, waren audio-opnames bij alle respondenten toegestaan, maar mochten ze alleen worden gebruikt voor het uitwerken van de interviews. Ze zijn daarom ook niet met derden gedeeld. De audio-opnames zijn ook direct na het uitwerken van de transcripties vernietigd. De interviewtranscripties zijn enkel met uiterst goede redenen op verzoek bij de onderzoeker te verkrijgen.

5.2 Conclusies

Aan de hand van resultaten uit het literatuuronderzoek en het empirisch onderzoek is het mogelijk om een conclusie te trekken en daarmee antwoord te geven op de centrale hoofdvraag, namelijk: ***"Welke beveiligingsmaatregelen uit het aandachtsgebied Identity & Access Management verlagen daadwerkelijk de kans op en impact van beveiligingsincidenten veroorzaakt door insider threats?"***

Uit de resultaten vanuit het literatuuronderzoek blijkt dat de meest voorkomende incidenten die door insider threats veroorzaakt worden, met name gericht zijn op het oneigenlijk gebruikmaken of het uitlekken van (vertrouwelijke) bedrijfsinformatie. Hierbij zijn insider threats te onderverdelen in twee categorieën, namelijk de bewuste gevallen en de onbewuste gevallen. Volgens de theorie ontstaan bewuste gevallen zich bij de juiste combinatie van motivatie en kansen die samen tot een actie leiden. Binnen de financiële sector is het met name de kans op financieel gewin dat tot actie leidt. Binnen andere sectoren is het motief niet altijd financieel van aard, maar wel bedoeld om op een bepaalde wijze een persoonlijk voordeel te behalen. Pas daarna volgen andere motieven zoals wraak, stress en bewuste sabotage.

Om de kans op en impact van beveiligingsincidenten te verlagen kunnen preventieve, detectieve, repressieve en correctieve maatregelen worden genomen. Het aandachtsgebied Identity & Access Management (IAM) heeft als doelstelling om ervoor te zorgen dat medewerkers altijd enkel en alleen geautoriseerd zijn tot hetgeen wat ze nodig hebben voor het kunnen uitvoeren van hun dagelijkse werkzaamheden. Maatregelen die bijdragen aan het beheersen van autorisaties zijn onder andere het proces voor het toekennen en herzien van alle uitgegeven autorisaties bij indiensttreding, interne verplaatsingen en uitdiensttreding, het scheiden van taken en verantwoordelijkheden bij kritische of fraudegevoelige handelingen, het toekennen van autorisaties op basis van functies en het periodiek rapporteren en uitvoeren van een herbeoordeling op alle uitgegeven autorisaties. Dit soort maatregelen hebben een positief effect op het verlagen van de kans op (langdurig) ongeoorloofd toegang tot informatie. In het geval dat een medewerker oneigenlijk gebruik maakt van informatie waar hij of zij met legitieme redenen toegang tot heeft, dan biedt IAM weinig tot geen detectieve en preventieve maatregelen om de kans en impact van dit soort incidenten te mitigeren. Met de kennis opgedaan in het literatuuronderzoek is het empirisch onderzoek gestart om de argumenten en theorieën betreffend de effectiviteit van IAM-maatregelen, zoals deze in de theorie gevonden zijn, aan de werkelijkheid te toetsen.

Voor het empirisch onderzoek is een meervoudige case study gedaan naar drie incidenten veroorzaakt door bewuste insider threats werkzaam binnen de financiële sector. De eerste van de onderzochte incidenten had zich voortgedaan bij een grote internationale vermogensbeheerder met tussen de 500 en 1000 medewerkers in Nederland. Hierbij verduisterde een medewerker miljoenen euro's door bij het afhandelen van de financiële transacties, bestemd voor de nabestaanden van de rekeninghouder, een deel van het vermogen naar andere bankrekeningen over te boeken. De andere twee incidenten hadden plaatsgevonden bij een grote internationale financiële dienstverlener met meer dan 1000 medewerkers in Nederland. De eerste van deze twee incidenten betreft een stagiair die na een felle woordenwisseling met zijn leidinggevende besloot om wraak te nemen en kritische bedrijfsinformatie te verwijderen. De derde van de onderzochte incidenten was veroorzaakt door een klantenservicemedewerker die klanten oplichtte en ze misleidde tot het overboeken van de betaling van hun openstaande facturen naar zijn eigen persoonlijke bankrekening.

In lijn met de theorie, vertonen twee van de drie onderzochte incidenten een motief van financieel gewin. Het andere incident is een overduidelijke wraakactie. Bij de onderzochte incidenten is geen motief van het bewust uitlekken of diefstal van vertrouwelijk bedrijfsinformatie geconstateerd.

Het door de daders veroorzaken van deze incidenten hangt samen met de algemene kans op een incident veroorzaakt door insider threats. In de drie onderzochte gevallen hebben de daders geen bedrijfsinformatie gebruikt naast hetgeen waartoe ze al geautoriseerd waren voor het kunnen uitvoeren van hun werkzaamheden. De daders hebben hierdoor geen ongeoorloofde (technische) middelen moeten gebruiken of andere medewerkers moeten betrekken om toegang te krijgen tot informatie, diensten of faciliteiten waarvoor ze niet geautoriseerd waren. Hierdoor hebben voor de hand liggende IAM-beveiligingsmaatregelen en principes zoals bijvoorbeeld het alleen uitgeven van de autorisaties vereist voor het kunnen uitvoeren van de dagelijks werkzaamheden, het toekennen van autorisaties op basis van functieprofielen en de periodieke herbeoordeling van alle uitgegeven autorisaties geen effect gehad op het daadwerkelijk verlagen van de kans op een dergelijk incident. Dit komt overeen met de resultaten van het literatuuronderzoek dat IAM weinig tot geen detectieve maatregelen biedt om de kans op een incident te verlagen in het geval dat een medewerker met legitieme redenen toegang tot de gebruikte bedrijfsinformatie heeft.

In twee van de drie gevallen was het detecteren dat iets niet in orde was niet het resultaat van technische hulpmiddelen, maar door meldingen van afwijkingen door personen. Bij het verwijderen van kritische bedrijfsinformatie merkte de afdeling klantenservice vrijwel direct op dat de informatie vereist voor het uitvoeren van de reguliere werkzaamheden miste. Kort daarna werd het incident onderzocht en de oorzaak dezelfde dag nog achterhaald. Het incident van het opzettelijk misleiden van klanten kwam aan het licht toen de betrokken klanten begonnen te klagen over het ontvangen van een betalingsherinnering terwijl ze de factuur vermeend al eerder hadden betaald. In het geval van het verduisteren van de gelden bestemd voor de nabestaanden van de rekeninghouder is het onduidelijk of detectie het gevolg was van oplettende klanten of dat het vanwege een geplande verbetering in de organisatie inrichting was. De verbetering in controles waren bijvoorbeeld het implementeren van het vierogenprincipe en functiescheiding tussen het invoeren en goedkeuren van financiële transacties. Het incident was met name mogelijk omdat tot daarvoor dit soort maatregelen niet geïmplementeerd waren. Bij de andere twee incidenten hadden deze maatregelen geen effect gehad vanwege dat het geen handelingen waren die over het algemeen als fraudegevoelig worden beschouwd en waarvoor dus meerdere individuen een goedkeuring voor zouden moeten geven. De preventieve IAM-beveiligingsmaatregelen vierogenprincipe en functiescheiding hebben dus zeker een positief effect om de kans te verlagen, mits ze relevant en toepasbaar zijn voor de situatie.

In de onderzochte gevallen hangt het motief van de dader nauw samen met de werkelijke impact op de organisatie. Waar het motief financieel van aard was, was de impact ook voornamelijk financieel. In de twee gevallen waar het motief financieel van aard was, hadden de organisaties de financiële schade na afloop aan de betrokken partijen vergoed. Doordat de incidenten niet het misbruik of het uitlekken van persoonsgegevens betreffen zijn de getroffen organisaties niet verplicht geweest om een melding bij de toezichthouder te doen. Ook is niets publiekelijk gecommuniceerd waardoor het imago van de getroffen organisaties geen schade heeft opgelopen. Het incident als gevolg van het verwijderen van kritische bedrijfsinformatie had ervoor gezorgd dat de organisatie voor een korte periode niet in staat was om haar klanten optimaal te bedienen. Vanuit de literatuur was opnieuw gebleken dat IAM weinig tot geen repressieve maatregelen biedt om de impact van incidenten veroorzaakt door insider threats te beperken wanneer een medewerker met legitieme redenen toegang tot informatie heeft. Indirect kan het wel bijdragen aan het beperken van de hoeveelheid bruikbare informatie een medewerker tegelijkertijd tot zijn of haar beschikking heeft. Bijvoorbeeld door het toepassen van data-abstractie, waar slechts een deel van de informatie zichtbaar is. Dit zou eventueel gecombineerd kunnen worden met Security Information & Event Management (SIEM) om direct afwijkingen te proberen te detecteren en daarmee zoveel mogelijk de impact te beperken.

De getroffen organisaties trekken soms ook lering uit de incidenten. Per incident verschilt het of na afloop ervan correctieve en/of preventieve maatregelen getroffen zijn om de schade te herstellen en de kans op of impact van een toekomstig soortgelijk incident te beperken. Na het ontdekken van het incident waar miljoenen euro's was verduisterd, had de organisatie in het geheim een speciaal team opgericht om passende preventieve oplossingen te bedenken en implementeren. Hierbij waren de mogelijke maatregelen niet beperkt tot een specifiek domein of aandachtsgebied. Het doel hierbij was betere en frequentere controles op alle afdelingen en type financiële transacties. In principe had de organisatie dus ervoor gezorgd dat ze niet langer een blinde vlek hadden zoals voorheen wel het geval was. Bij het verwijderen van kritische bedrijfsinformatie heeft de getroffen organisatie hiervoor geen nieuwe preventieve maatregelen geïmplementeerd. Zij achtten hun correctieve maatregelen zoals het snel en volledig kunnen herstellen van data op basis van back-ups als voldoende hiervoor. De organisatie had dan ook niet meer dan een paar uur last van het dataverlies. Bij het laatste incident ging het vooral om de communicatie tussen de organisatie en haar klanten. Toch heeft de getroffen organisatie aangegeven geen nieuwe maatregelen te willen implementeren. Hierdoor is de organisatie eigenlijk nog steeds kwetsbaar voor hetzelfde soort incident.

Concluderend en alles overwegend hebben de beveiligingsmaatregelen uit het aandachtsgebied van Identity & Access Management een wisselend effect op het daadwerkelijk verlagen van de kans op en impact van beveiligingsincidenten die veroorzaakt worden door insider threats. De theorie en de praktijk wijzen beiden uit dat bepaalde IAM-maatregelen, zoals de periodieke herbeoordeling van alle uitgegeven autorisaties en het herzien van autorisaties bij interne verplaatsingen, een positief effect hebben op het voorkomen dat medewerkers toegang krijgen tot vertrouwelijke bedrijfsinformatie die niet relevant is voor het uitvoeren van hun dagelijkse werkzaamheden. Ook het onbedoeld en ongewenst stapelen van conflicterende autorisaties, zodat een medewerker bijvoorbeeld in staat is om zelfstandig een factuur te kunnen invoeren en goedkeuren, kan hiermee worden voorkomen. Preventieve maatregelen zoals het vierogenprincipe en het scheiden van taken en bevoegdheden bij kritische en fraudegevoelige handelingen hebben ook een positief effect op het voorkomen dat een medewerker die alleen handelt in staat is om misbruik van informatie te maken.

In de tabel hieronder zijn de IAM-beveiligingsmaatregelen afgezet tegen de onderzochte cases. Van elke maatregel is de mate van effectiviteit bepaald voor het (potentieel) verlagen van de kans op en impact van het incident. Variërend van niet effectief, enigszins effectief, effectief tot zeer effectief. Met uitzondering van de eerste case, toont de tabel opnieuw aan dat IAM in feite maar weinig tot geen effectieve maatregelen biedt op het moment dat een medewerker met legitieme redenen, bijvoorbeeld vanwege hun rol of functie, toegang heeft tot alle informatie die nodig is om misbruik van de situatie te kunnen maken.

Tabel 3: De effectiviteit van IAM-beveiligingsmaatregelen in de onderzochte cases

IAM-beveiligingsmaatregelen	**Case 1** *Verduisteren van miljoenen euro's*	**Case 2** *Verwijderen van kritische informatie*	**Case 3** *Misleidende communicatie*
Toekennen van autorisaties op basis van vooraf gedefinieerde functieprofielen	Effectief (+)	Enigszins effectief (+/-)	Niet effectief (--)
Periodiek beoordelen van alle uitgegeven autorisaties (bijvoorbeeld elk kwartaal)	Niet effectief (--)	Niet effectief (--)	Niet effectief (--)
Herzien van alle uitgegeven autorisaties bij functiewijzigingen en uitdiensttreding	Enigszins effectief (+/-)	Niet effectief (--)	Niet effectief (--)
Het scheiden van kritische taken en verantwoordelijkheden	Zeer effectief (++)	Niet effectief (--)	Niet effectief (--)
Toepassen van het vierogenprincipe bij kritische of fraudegevoelige handelingen	Zeer effectief (++)	Enigszins effectief (+/-)	Effectief (+)
Het monitoren en beperken van het gebruik van beheer- en serviceaccounts	Niet effectief (--)	Niet effectief (--)	Niet effectief (--)

5.3 Aanbevelingen voor de praktijk

Volgens het literatuuronderzoek zien organisaties de maatregelen uit het aandachtsgebied van IAM als één van de mogelijke oplossingen tegen insider threats. Uit dit onderzoek blijkt het inderdaad zo dat de maatregelen uit het aandachtsgebied van IAM een positief effect hebben op het voorkomen dat onbevoegden toegang krijgen tot vertrouwelijke bedrijfsinformatie. Een organisatie doet daarom goed eraan om eerst de basis van IAM op orde te hebben. Dit begint met het implementeren van de meest basale IAM-principes zoals het alleen uitgegeven autorisaties die vereist zijn voor het kunnen uitvoeren van de werkzaamheden. Een hulpmiddel hierbij is het definiëren van functieprofielen met de bijbehorende autorisaties. Dit draagt bij aan de basis door autorisaties per functies te bepalen en op voorhand conflicterende autorisaties te identificeren en kritische en/of fraudegevoelige taken, bevoegdheden en verantwoordelijkheden te scheiden.

Echter, op het moment dat een medewerker met legitieme redenen toegang heeft tot vertrouwelijke bedrijfsinformatie, is de effectiviteit van IAM-maatregelen vrij beperkt. In dit soort gevallen is het noodzakelijk om IAM te combineren met andere soorten maatregelen en technieken om de kans op een incident door een insider threat te kunnen verlagen. Hiervoor zou gekeken moeten worden naar oplossingen en maatregelen die samenvallen met de principes en uitgangspunten van IAM. Zoals het toepassen van data-abstractie waardoor bijvoorbeeld klantenservicemedewerkers wel inzicht krijgen in de NAW-gegevens van klanten, maar de vertrouwelijke of fraudegevoelige gegevens zoals het BSN-nummer afgeschermd worden, tenzij het (tijdelijk) nodig is voor het kunnen uitvoeren van de werkzaamheden. Andere mogelijkheden zijn het direct en continu monitoren op afwijkingen in de bedrijfsvoering met slimme oplossingen zoals Data Loss Prevention en Security Information & Event Management (SIEM).

Het verlagen van de kans op een bewuste insider threat kan ook met niet-technische oplossingen. Uit het literatuuronderzoek en de case study is gebleken dat het motief in de financiële sector vaak het persoonlijke financiële gewin is. De overweging of verleiding om tot actie over te gaan hangt nauw samen met drie factoren, namelijk de vereiste inspanning, de eventuele risico's (zoals de pakkans) en de verwachte opbrengsten. Door deze factoren te beïnvloeden, bijvoorbeeld door als organisatie de risico's en consequenties veel prominenter te benadrukken, kan dit potentieel een afschrikkend effect hebben op de overweging van een insider threat om daadwerkelijk tot actie over te gaan.

5.4 Aanbevelingen voor verder onderzoek

Dit onderzoek geeft inzicht in de effectiviteit van beveiligingsmaatregelen uit het aandachtsgebied van IAM op insider threats. Echter, de case study is beperkt tot drie cases van de vele cases die zich jaarlijks binnen de financiële sector voordoen. Een vervolgonderzoek zou de opzet van dit onderzoek als een basis kunnen nemen om een grotere populatie van cases te analyseren en zo een completer beeld te krijgen van het type incidenten veroorzaakt door insider threats binnen de financiële sector.

Eén van de onderdelen die in dit onderzoek in beperkte mate is onderzocht, is het perspectief van de dader. Alle cases zijn voornamelijk bekeken vanuit het perspectief van de getroffen organisatie. Door de aanpak aan te passen en in een vervolgonderzoek de cases vanuit het perspectief van de dader te onderzoeken zou meer inzicht verkregen kunnen worden in de psychologie aspecten die een rol hebben gespeeld. Dit zou kunnen leiden tot het definiëren van niet-technologische maatregelen die de kans op een insider threat kunnen verlagen.

Tot slot zou dezelfde case study opzet ook binnen andere sectoren kunnen worden uitgevoerd. In de financiële sector is het financieel gewin een veelvoorkomend motief. Echter, de motieven in andere sectoren zijn mogelijk heel anders van aard en kunnen dus ook hele andere oorzaken en gevolgen hebben voor de getroffen organisatie.

Referenties

Alsaawi, A. (2014). A Critical Review of Qualitative Interviews. *European Journal of Business and Social Sciences, 3*, 149-156. doi:http://doi.org/10.2139/ssrn.2819536

Atkinson, J. (2002). Four steps to analyse data from a case study method. *ACIS 2002 Proceedings*, 38.

Aven, T. (2013). A conceptual framework for linking risk and the elements of the data–information–knowledge–wisdom (DIKW) hierarchy. *Reliability Engineering & System Safety, 111*, 30-36. doi:https://doi.org/10.1016/j.ress.2012.09.014

Calder, A. (2013). *ISO27001 / ISO27002: A Pocket Guide*. London: IT Governance.

Campbell, J. L., Quincy, C., Osserman, J., & Pedersen, O. K. (2013). Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. *Sociological Methods & Research, 42*(3), 294-320. doi:10.1177/0049124113500475

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Boston, MA: Addison Wesley Professional.

Cisco. (2014). Data Leakage Worldwide: Common Risks and Mistakes Employees Make. Retrieved November 4, 2018 from https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html

Clarke, N. L., & Furnell, S. M. (2007). Advanced user authentication for mobile devices. *Computers & Security, 26*(2), 109-119.

Cole, E. (2017). Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey. Retrieved September 22, 2018 from https://www.sans.org/reading-room/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890

Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal, 33*(4), 425-435. doi:10.1108/MAJ-11-2017-1692

Custers, B. H. M., Dechesne, F., Georgieva, I. N., & Hof, S. (2017). *De bescherming van persoonsgegevens: Acht Europese landen vergeleken*. Den Haag: Sdu Uitgevers.

Dinoor, S. (2010). Privileged identity management: securing the enterprise. *Network Security, 2010*(12), 4-6. doi:10.1016/S1353-4858(10)70144-6

Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing Insider Threat Risk with Behavioral Monitoring. *Review of Business, 38*(2).

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107-115. doi:10.1111/j.1365-2648.2007.04569.x

Everett, C. (2011). Identity and Access Management: the second wave. *Computer Fraud & Security, 2011*(5), 11-13. doi:10.1016/s1361-3723(11)70051-3

FBI. (2011). Chinese National Sentenced for Stealing Ford Trade Secrets. Retrieved November 4, 2018 from https://archives.fbi.gov/archives/detroit/press-releases/2011/de041211.htm

Fuchs, L., & Pernul, G. (2012). Minimizing insider misuse through secure Identity Management. *Security and Communication Networks, 5*(8), 847-862. doi:10.1002/sec.314

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404-410. doi:https://doi.org/10.1016/j.im.2009.06.005

Gunter, C. A., Liebovitz, D., & Malin, B. (2011). Experience-based access management: A life-cycle framework for identity and access management systems. *IEEE security & privacy, 9*(5), 48.

Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers, 15*(1), 1-4. doi:10.1007/s10796-013-9419-8

The Insider Threat. (2017). *Computer Fraud & Security, 2017*(8), 1. doi:10.1016/s1361-3723(17)30063-5

Koch, M., & Möslein, K. M. (2005). Identities management for e-commerce and collaboration applications. *International Journal of Electronic Commerce, 9*(3), 11-29.

Kroeks-de, R. C. C. M., Westerdijk, R. J. J., & Zwenne, G. J. (2016). De Algemene Verordening Gegevensbescherming. *Tijdschrift voor Internetrecht, 2016*, 9.

Lawler, R. (2017). Judge Denies Uber's Request for Stay in Waymo Suit. Retrieved November 4, 2018 from https://techcrunch.com/2017/06/07/uber-waymo-lawsuit-stay-denied

Lewis, N. (2012). Access rights – protect access to your data or lose it: serious misconceptions about information security. *Computer Fraud & Security, 2012*(11), 8-10. doi:https://doi.org/10.1016/S1361-3723(12)70113-6

Liu, X., & Murphy, D. (2015). They Are Not All Enemies: Detecting and Deterring Non-Malicious, Privileged IT User Threat Using an interdepartmental Approach. *SAIS 2015 PROCEEDINGS*, 14. https://aisel.aisnet.org/sais2015/14

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security, 24*(5), 371-380. doi:https://doi.org/10.1016/j.cose.2004.10.003

Manders-Huits, N. (2010). Practical versus moral identities in identity management. *Ethics and Information Technology, 12*(1), 43-55. doi:10.1007/s10676-010-9216-8

Miles, M. B., & Huberman, M. A. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. Thousand Oaks, CA: SAGE Publications.

Miller, S. (2016). 2016 U.S. State of Cybercrime Highlights. Retrieved November 4, 2018 from https://insights.sei.cmu.edu/insider-threat/2017/01/2016-us-state-of-cybercrime-highlights.html

Moscaritolo, A. (2009). Disgruntled Fannie Mae Insider Indicted for Cyber Intrusion. Retrieved November 4, 2018 from https://www.scmagazine.com/home/security-news/disgruntled-fannie-mae-insider-indicted-for-cyber-intrusion/

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems, 92*, 47-56. doi:https://doi.org/10.1016/j.dss.2016.09.012

Perkins, E. L., & Allan, A. (2005). Consider identity and access management as a process, not a technology. *Gartner Report*(G00129998).

Raisel, E. M. (1998). *The McKinsey Way: Using the Ways of the World's Top Strategic Consultants to Help You and Your Business*. New York: McGraw-Hill.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29*(2), 38-47.

Schulze, H. (2018). Insider Threat Report: 2018. Retrieved September 22, 2018 from https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

Sokolowski, J. A., Banks, C. M., Dover, T. J. J. C., & Theory, M. O. (2016). An agent-based approach to modeling insider threat. *Computational and Mathematical Organization Theory, 22*(3), 273-287. doi:10.1007/s10588-016-9220-6

Tankard, C. (2015). Data classification – the foundation of information security. *Network Security, 2015*(5), 8-11. doi:https://doi.org/10.1016/S1353-4858(15)30038-6

van den Berg, J. (2015). Wat maakt cyber security anders dan informatiebeveiliging? *Magazine Nationale Veiligheid en Crisisbeheersing*(2), 4-5.

Verheij, M. (2016). Datalekken. *Vakblad Sociaal Werk, 17*(4), 37-39.

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal, 26*(2), 107-124. doi:10.1057/sj.2012.1

Wilber, D. Q. (2016). So Began a 20-Year Course of Conduct of Lying, Cheating, and Stealing. Retrieved November 4, 2018 from http://www.pressreader.com/Canada/bloomberg-businessweek-north-america/20160208/282286729303079/

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly, 37*(1).

Witty, R. J., Allan, A., Enck, J., & Wagner, R. (2003). Identity and access management defined. *Research Study SPA-21-3430, Gartner.*

Yin, R. K. (2014). *Case Study Research*. Thousand Oaks, CA: SAGE Publications.

Bijlage A: Interviewvragen

Algemeen

1. Wat is uw functie en wat zijn uw primaire werkzaamheden?
2. Wat is de primaire doelstelling van uw organisatie?
3. Hoeveel medewerkers zijn werkzaam bij uw organisatie?

Informatiebeveiligingsbeleid

4. Heeft uw organisatie een overkoepelend informatiebeveiligingsbeleid die van toepassing is op alle organisatieonderdelen?
5. Is het informatiebeveiligingsbeleid van uw organisatie door het management geaccordeerd?
6. Is het informatiebeveiligingsbeleid gebaseerd op een norm zoals bijvoorbeeld de ISO27001?
7. Wanneer is het informatiebeveiligingsbeleid voor het laatst bijgewerkt?
8. Hoe is het informatiebeveiligingsbeleid aan de medewerkers werkzaam bij uw organisatie beschikbaar gesteld?

Casuïstiek: Situatie

9. Wat voor incident heeft zich plaatsgevonden?
10. Wat voor soort informatie was betrokken bij dit incident?
11. Hoe was dit soort informatie intern geclassificeerd?
12. Wat voor functie vervulde de dader van dit incident?
13. Wat voor dienstverband had de dader?
14. Had de dader voor zijn of haar functie toegang tot deze informatie horen te hebben?
15. Zo niet, hoe was de dader dan op de hoogte van het bestaan van deze informatie?
16. Had de dader een speciaal account gebruikt, zoals een beheer- of serviceaccount?
17. Waar deed dit incident zich voor? (Bijvoorbeeld op kantoor, thuis of een externe werklocatie)
18. Hoelang geleden heeft dit incident plaatsgevonden?

Casuïstiek: Motivatie

19. Wat was of wat denkt u dat het doel van de dader was?
20. Wat voor (potentieel) gewin had de dader met dit incident kunnen krijgen?
21. Hoe was de verhouding tussen de dader en zijn of haar leidinggevende?
22. Hoe was de verhouding tussen de dader en andere medewerkers binnen het team?
23. Wat voor risico's heeft de dader (mogelijk) moeten nemen?
24. Was dit het enige incident van de dader?

Casuïstiek: Detectie

25. Was vooraf aan dit incident al een vermoeden van wangedrag bij de dader?
26. Hoe en wanneer was dit incident daadwerkelijk ontdekt?
27. Hoe kan het zijn dat dit incident niet eerder was ontdekt?
28. Hoeveel tijd zat tussen het begin van het oneigenlijk gebruik maken van informatie en het daadwerkelijk ontdekken ervan?
29. Heeft uw organisatie op dit moment al IAM-gerelateerde maatregelen geïmplementeerd zoals onder andere, functiescheiding, (de-)autorisatie als gevolg van een functiewijziging en/of een periodieke herbeoordeling van alle uitgegeven autorisaties?
30. Had dit incident, naar uw mening, voorkomen kunnen worden door het (beter) inrichten van IAM-maatregelen?
31. Had dit incident, naar uw mening, voorkomen kunnen worden door het (beter) inrichten van andere informatiebeveiligingsmaatregelen?

Casuïstiek: Impact

32. Wat was de (financiële) impact van dit incident?
33. Heeft dit incident tot negatieve publiciteit geleid?
34. Wat was (potentieel) de impact van dit incident indien het later of geheel niet was ontdekt?
35. Heeft uw organisatie aangifte gedaan van dit incident?
36. Wat voor consequenties had dit incident voor de dader?

Casuïstiek: Repressie

37. Wat voor repressieve maatregelen had uw organisatie ingericht die de gevolgen en impact van het incident hebben beperkt?
38. Wat voor repressieve maatregelen had uw organisatie ingericht die de gevolgen en impact hadden moeten beperken, maar in dit geval niet voldoende waren?

Casuïstiek: Afhandeling en correctie

39. Wat voor maatregelen heeft uw organisatie sinds dit incident genomen om voortaan dit soort incidenten te voorkomen en/of (eerder te) detecteren?
40. Heeft uw organisatie maatregelen getroffen om de vereiste inspanning, te nemen risico's en/of (verwachte) opbrengsten van soortgelijke incidenten te beïnvloeden?
41. Heeft u het gevoel dat uw organisatie op dit moment voldoende is voorbereid op de komst van toekomstige insider threats?
42. Zo ja, wat voor maatregelen heeft u genomen om uw organisatie te beschermen tegen de toekomstige insider threats?
43. Wat voor preventieve en detectieve maatregelen zou uw organisatie verder moeten nemen om de kans op incidenten veroorzaakt door insider threats te verlagen?
44. Wat voor repressieve maatregelen zou uw organisatie moeten nemen om de gevolgen en impact van dit soort incidenten in de toekomst te verlagen?

Bijlage B: Protocol voor het afnemen van interviews

Voor het afnemen van de interviews is een protocol gehanteerd dat hieronder verder is toegelicht. De respondenten kwamen allemaal uit het eigen netwerk of zijn aangedragen door iemand uit het eigen netwerk. Hierdoor zijn de respondenten eerst telefonisch benaderd om vooraf mondeling de aanleiding van het interview toe te lichten. Tijdens het telefoongesprek is de respondent gevraagd naar de ervaring met een case die voldoet aan de criteria van het onderzoek. Ook is gelijk telefonisch een afspraak ingepland voor het interview. Direct na het telefoongesprek is aan de respondent een email verstuurd met een samenvatting van de besproken onderwerpen waaronder:

- de aanleiding van het onderzoek en de onderzoeksvraag;
- een beschrijving van het begrip 'insider threat';
- uitleg over de twee delen van het onderzoek (literatuuronderzoek en empirisch onderzoek);
- criteria voor een geschikte case;
- een samenvatting van de gewenst informatie;
- de wijze waarop de resultaten verwerkt worden;
- bevestiging dat de resultaten anoniem worden gepubliceerd.

Alle interviews zijn afgenomen op het kantoor van de standplaats van de respondent tijdens een één op één sessie. Vooraf aan het beginnen van het interview zijn de onderwerpen uit de email opnieuw toegelicht. De interviews zijn met behulp van de spraakrecorder applicatie op de mobiele telefoon van de onderzoeker opgenomen en na het gesprek uitgewerkt tot een interviewtranscriptie. Tijdens het interview had de onderzoeker de vragenlijst afgedrukt en naast zich beschikbaar. De respondent heeft zowel voor, als tijdens, als na het gesprek geen inzicht gekregen in de vragen uit de vragenlijst. Twee van de vier respondenten gaven aan de transcriptie na afloop te willen ontvangen. Wijzigingen in de transcripties waren niet mogelijk vanwege het woordelijk uitwerken van de transcripties. Kort na het uitwerken van de interviewtranscripties zijn ze allemaal gecodeerd aan de hand van het protocol voor het coderen van interviews. Een overzicht van de afgenomen interviews, de functies van de respondenten en een omschrijving van het interview is in de tabel hieronder opgenomen.

Tabel: Overzicht interviews

Referentie	Datum	Respondent	Omschrijving
Interview A	03-05-2019	Medewerker informatiemanagement	Interview over case study 1. Gaat inhoudelijk over de case en de beveiligingsmaatregelen die destijds waren ingericht.
Interview B1	06-05-2019	Medewerker fraudezaken	Interview over case study 2. Gaat inhoudelijk over de gebeurtenissen rondom de case zelf, maar niet over de beveiligingsmaatregelen ten tijde van het incident.
Interview B2	06-05-2019	Functionaris informatiebeveiliging	Interview over case study 2. Specifiek gericht op de beveiligingsmaatregelen ten tijde van het incident.
Interview C	09-05-2019	Medewerker fraudezaken	Interview over case study 3. Inhoudelijk over de case zelf. De beveiligingsmaatregelen uit het interview B2 zijn ook op deze case van toepassing.

Bijlage C: Protocol voor het coderen van interviews

Voor het analyseren en coderen van de interviewtranscripties is gebruik gemaakt van het kwalitatief analyseprogramma ATLAS.ti. Nog voordat de transcripties waren uitgewerkt, zijn de codes bestemd voor het open coderen opgesteld. Echter, tijdens het open coderen was het al snel duidelijk dat de initiële lijst met codes onvoldoende was om effectief te coderen. Zodoende zijn tijdens het open coderen nog additionele codes toegevoegd. Hieronder volgt een lijst van de codes gebruikt voor het open coderen. De codes gemarkeerd met een ster zijn later in het coderingsproces toegevoegd:

Overzicht van codes gebruikt tijdens het open coderen

- Consequenties dader *
- Correctie
- Detectie
- Financiële impact
- Informatiebeveiligingsbeleid *
- Inrichting informatiebeveiliging
- Motivatie
- Niet-financiële impact
- Organisatiecontext
- Relatie *
- Repressie
- Risico's *
- Situatie

De transcripties zijn eerst los van elkaar gecodeerd door de fragmenten in de transcripties met de bovenstaande codes te labelen. Dit is opgevolgd door het axiaal coderen, waarbij de fragmenten en codes opnieuw zijn doorgelopen om onderscheid te maken tussen de hoofd- en subthema's. Hierbij zijn de interviewtranscripties ook onderling met elkaar vergeleken. Het resultaat hiervan is de lijst die hieronder is weergegeven. Nieuwe en gewijzigde codes ten opzichte van tijdens het open coderen zijn aangeduid met een ster:

Overzicht van codes als gevolg van het axiaal coderen

- Correctie
- Consequenties dader
- Detectie
- Impact *
    - Financiële impact
    - Niet-financiële impact
- Informatiebeveiligingsbeleid
- Interne communicatie *
- Inrichting informatiebeveiliging
- Motivatie
- Organisatiecontext
- Relatie
- Repressie
- Risico's
- Situatie
    - Beschrijving uitvoering *
    - Frequentie incidenten *
    - Kenmerken dader *
    - Type informatie *
    - Uitvoeringsperiode *

Op basis van de tekstfragmenten die dezelfde codes hebben, is het proces van selectief coderen uitgevoerd. Hierbij zijn verbanden gelegd tussen de fragmenten onderling en tussen de verschillende cases. Hierbij zijn geen nieuwe codes opgesteld, opgesplitst en/of verwijderd. Het resultaat van het open coderen zijn de uitgewerkte resultaten per thema.